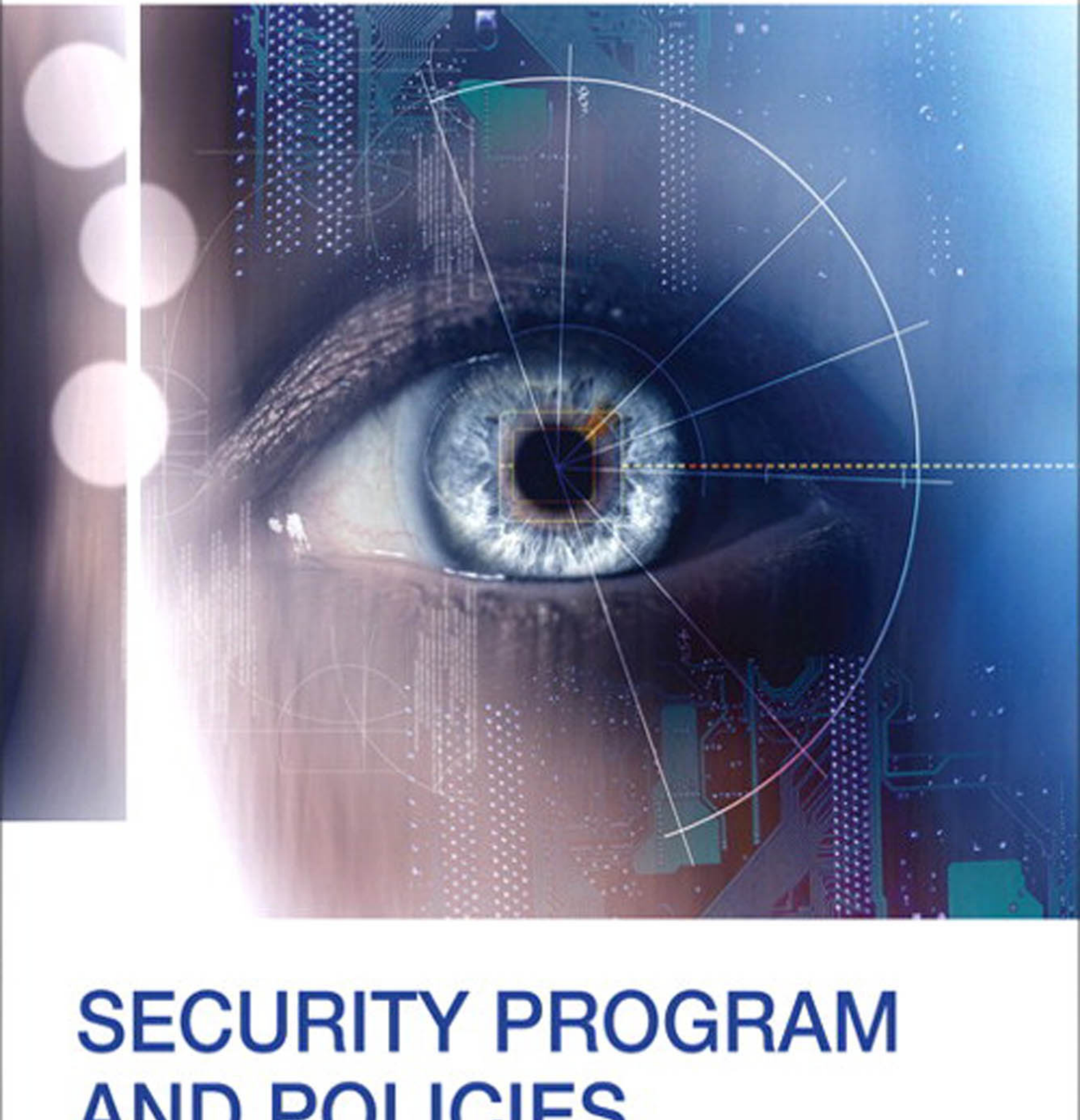


SECURITY PROGRAM AND POLICIES

PRINCIPLES AND PRACTICES

SARI STERN GREENE

Security Program and Policies: Principles and Practices

Second Edition

Sari Stern Greene

PEARSON
IT CERTIFICATION

800 East 96th Street, Indianapolis, Indiana 46240 USA

Security Program and Policies: Principles and Practices, Second Edition

Sari Stern Greene

ISBN-13: 978-0-7897-5167-6
ISBN-10: 0-7897-5167-4

Library of Congress Control Number: 2014932766

Printed in the United States of America

Second Printing: July 2015

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Editor-in-Chief
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Box Twelve, Inc.

Managing Editor
Sandra Schroeder

Project Editor
Seth Kerney

Copy Editor
Bart Reed

Indexer
Heather McNeill

Proofreader
Anne Goebel

Technical Editors
Ronald Gonzales
Tatyana Zidarov

Publishing Coordinator
Vanessa Evans

Interior Designer
Gary Adair

Cover Designer
Mark Shirar

Compositor
Studio Galou, LLC

Contents at a Glance

Table of Contents

About the Author

Sari Greene is an information security practitioner, author, and entrepreneur. She founded Sage Data Security in 2002 and has amassed thousands of hours in the field working with a spectrum of technical, operational, and management personnel as well as board of directors, regulators, and service providers.

Sari provided expert witness testimony in the groundbreaking PATCO v. Ocean National Bank case. From 2006 through 2010, she served as the managing director for the MEAPC, a coalition of 24 financial institutions that embrace a mission of preventing information theft and fraud through public education and awareness. Since 2010, she has served as the chair of the annual Cybercrime Symposium held in Portsmouth, New Hampshire.

Sari's first text was *Tools and Techniques for Securing Microsoft Networks*, commissioned by Microsoft to train its partner channel, followed soon after by the first edition of *Security Policies and Procedures: Principles and Practices*. She has published a number of articles and whitepapers related to information security and has been quoted in *The New York Times*, *Wall Street Journal*, CNN, and on CNBC. She speaks regularly at security conferences and workshops around the country and is a frequent guest lecturer.

Sari has an MBA from the University of New Hampshire system and has earned an array of government and industry certifications and accreditations, including ISACA Certification in Risk and Information Systems Control (CRISC), ISACA Certification in Security Management (CISM), ISC^2 Certification in Information Systems Security (CISSP), and Microsoft Certified Network Engineer (MCSE), and is certified by the National Security Agency to conduct NSA-IAM assessments for federal government agencies and contractors.

You can contact Sari at sari@sarigreene.com or follow her on Twitter @sari_greene.

Dedication

To all who honor the public trust.

Acknowledgments

Transforming raw material into a useful publication is a team effort. My colleagues at Sage Data Security generously and passionately shared their knowledge. Dr. Ron Gonzales of National University and Tatyana Zidarov of Kaplan University provided thoughtful feedback and recommendations. Senior Development Editor Chris Cleveland and Development Editor Jeff Riley expertly guided the process. The Fadiman family made available a wonderful workspace. The Captain, as always, waited patiently. To all, I am grateful.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book. Preface

Preface

More than two billion people use the Internet for research, banking, shopping, travel, job searches, social media, and conducting business. The rate of connectivity is estimated to be growing at a rate of eight new users every second. We live in a truly amazing world where, with a click of a mouse, ideas can be shared across continents and cultures. From global politics to delicate telesurgery, this ability to share information has profoundly and positively impacted our world. As wonderful as the interconnectivity is, however, there is a real and present danger. At risk is the confidentiality, integrity, and availability of the critical infrastructure that we have come to depend upon to run our lives, our economy, and our governments.

Information security has taken on a new urgency. As security professionals, we have an obligation to design, adopt, influence, and implement environments that protect information and information systems from misuse. Information security is more than an activity and more than a profession—it is a civic duty. Each of us as individuals, organizations, institutions, and governments are entrusted with information. It is our job to honor that trust. This book focuses on achieving that goal.

Information security issues have been studied and deliberated worldwide. The International Organization for Standardization (ISO) has developed and published information security standards referred to as the ISO 27002:2013—Code of Practice for Information Security Management. This code of practice provides a framework for developing information security policies and understanding information security controls. Throughout this book, we reference the ISO 27002:2013 standard. It must be noted that we are using the standard as a framework, and that this book is not to be construed as an official interpretation of the ISO 27002:2013. Organizations that choose to implement the standard should purchase the complete document from the ISO (www.iso.ch). In addition to the ISO standards, this text incorporates guidance from the United States National Institute of Standards and Technology (NIST). NIST Special Publications are referenced in each chapter. The publications are available online and can be downloaded at no charge. A complete list of the Special Publications referenced in this text can be found in Appendix A, "Information Security Program Resources."

Security Programs and Policies: Principles and Practices is conceptually divided into three parts. Part I (Chapters 1 and 2) is designed to provide the foundation for developing, introducing, and implementing policies. Part II (Chapters 3-12) dives deep into information security program components, principles, and policies across multiple security domains. Part III (Chapters 13-15) is a practical application of information security practices in regard to compliance with federal regulations as well as industry best practices.

Included in the Appendixes are two policy documents. Appendix B, "Sample Information Security Policy," is a comprehensive information security policy document that incorporates all of the information security program components and principles discussed throughout the text. Appendix C is a sample Information Systems Acceptable Use Agreement and Policy. Readers are encouraged to customize these documents and use them in their organizations.

The responsibility for information security does not rest with a single role. This book is intended for anyone who is preparing for a leadership position in business, government, academia, or healthcare. Before embarking on a study of information security, students should have an understanding of the role of information systems in the business world and basic network infrastructure design. Mastering the information presented in this book is a must for information security professionals

Dedication

To all who honor the public trust.

Acknowledgments

Transforming raw material into a useful publication is a team effort. My colleagues at Sage Data Security generously and passionately shared their knowledge. Dr. Ron Gonzales of National University and Tatyana Zidarov of Kaplan University provided thoughtful feedback and recommendations. Senior Development Editor Chris Cleveland and Development Editor Jeff Riley expertly guided the process. The Fadiman family made available a wonderful workspace. The Captain, as always, waited patiently. To all, I am grateful.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

This page intentionally left blank

Chapter 1

Understanding Policy

Chapter Objectives

After reading this chapter and completing the exercises, you should be able to do the following:

- Describe the significance of policies.
- Evaluate the role policy plays in corporate culture and civil society.
- Articulate the objective of information security–related policies.
- Identify the seven characteristics of successful policies.
- Define the lifecycle of an information security policy.

We live in an interconnected world where individual as well as collective actions have the potential to result in inspiring goodness or tragic harm. The objective of Information Security is to protect each of us, our economy, our critical infrastructure, and our country from the harm that can result from inadvertent or intentional misuse, compromise, or destruction of information and information systems. The United States Department of Homeland Security defines critical infrastructure sectors as agriculture, food, water, public health, emergency services, government, defense industrial base, information technology and telecommunications, energy, transportation, banking, finance, chemical industry, and postal and shipping. The services provided by critical infrastructure sectors are "the backbone of our nation's economy, security and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1]

FYI: National Security

Presidential Policy Directive 7 – Protecting Critical Infrastructure (2003) established a national policy that required federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from physical and cyber terrorist attacks. The directive acknowledged that it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, but that strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.

Ten years later, in 2013, *Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience* broadened the effort to strengthen and maintain secure, functioning, and resilient critical infrastructure by recognizing that this endeavor is a shared responsibility among the federal, state, local, tribal, and territorial entities as well as public and private owners and operators of critical infrastructure.

Policy is the seminal tool used to protect both our critical infrastructure and our individual liberties. The role of policy is to provide direction and structure. Policies are the foundation of companies' operations, a society's rule of law, or a government's posture in the world. Without policies, we would live in a state of chaos and uncertainty. The impact of a policy can be positive or negative. The hallmark of a positive policy is one that supports our endeavors, responds to a changing environment, and potentially creates a better world.

In this chapter, we will explore policies from a historical perspective, talk about how humankind has been affected, and learn how societies have evolved using policies to establish order and protect people and resources. We will apply these concepts to information security principles and policies. We will discuss in detail the seven characteristics of an effective information security policy. We will acknowledge the influence of government regulation on the development and adoption of information security policies and practices. Lastly, we will tour the policy lifecycle.

Looking at Policy Through the Ages

Sometimes an idea seems more credible if we begin with an understanding that it has been around for a long time and has withstood the test of time. Since the beginning of social structure, people have sought to form order out of perceived chaos and to find ways to sustain ideas that benefit the advancement and improvement of a social structure. The best way we have found yet is in recognizing our common problems and finding ways to avoid causing or experiencing them in our future endeavors. Policies, laws, codes of justice, and other such documents came into existence almost as soon as alphabets and the written word allowed them. This does not mean that before the written word there were no policies or laws. It does mean that we have no reference to spoken policy known as "oral law," so we will confine our discussion to written documents we know existed and still exist.

FYI: Life in Ancient Times

It might be helpful to understand what life was like around 1000 B.C.E. Picture yourself in a world with rampant and uncontrolled disease, crime, social unrest, poverty, and superstition—a world where the rules people lived by were arbitrary, decided in the moment, driven by reactionary instinct, or dictated by some mystical superstition without any basis in fact.

Now consider our own society. Disease is largely controlled, or at least treated with, medicine. Crime is controlled through a justice system, including written law enforced by police and upheld and adjudicated by a judicial system, in which convicted offenders are punished in a penitentiary system. In further contrast, social unrest is built into our system of free speech, poverty is managed with varying degrees of success by a social welfare system, and superstition has largely given way to science, as we understand more and more of our world.

We are going to look back through time at some examples of written policies that had and still have a profound effect on societies across the globe, including our own. We are not going to concern ourselves with the function of these documents. Rather, we will begin by noting the basic commonality we can see in the why and how they were created to serve a larger social order. Some are called laws, some codes, and some canons, but what they all have in common is that they were created out of a perceived need to guide human behavior in foreseeable circumstances, and even to guide human behavior when circumstances could not be or were not foreseeable. Equal to the goal of policy to sustain order and protection is the absolute requirement that our policy be changeable in response to dynamic conditions.

The Bible as Ancient Policy

Let's start by going back in time 3,300 years and look at one of the earliest examples of written policy still in existence: the Torah. For those of the Jewish faith, the Torah is the Five Books of Moses. Christians refer to the Torah as the Old Testament of the Bible. If we put aside the religious aspects of this work, we can examine the Torah's importance from a social perspective and its lasting impact on the entire world. The Torah articulated a codified social order. It contains rules for living as a member of a social structure. The rules were and are intended to provide guidance for behavior, the choices people make, and their interaction with each other and society as a whole. Some of the business-related rules of the Torah include the following:

- Not to use false weights and measures
- Not to charge excessive interest
- To be honest in all dealings
- To pay wages promptly
- To fulfill promises to others

These are behavior directives—or what we now refer to as policies. We can clearly see similarities between these ancient social rules and our modern social standards. As mentioned earlier, we are not concerned with the content of these ancient documents as much as the reason for their creation. The various common experiences of all peoples led to common behaviors and choices, which all too often led to the ills plaguing their social systems. With careful thought, clearly stated and communicated in written form, many of these social problems could be avoided by giving people rules to guide them through their daily lives. Any person who could follow these rules would certainly find life easier to navigate. Moreover, if *everyone* followed the rules, the entire community would become more stable. Time previously spent avoiding problems could instead be spent improving the community.

The United States Constitution as a Policy Revolution

Let's look at a document with which you may be a little more familiar: the Constitution of the United States of America. The Constitution is a collection of articles and amendments codifying all aspects of American government and citizens' rights. The articles themselves are very broad principles that recognize that the world will change. This is where the amendments play their role as additions to the original document. Through time, these amendments have extended rights to more and more Americans and have allowed for circumstances our founders could not have foreseen. The founders wisely built into the framework of the document a process for changing it while still adhering to its fundamental tenets. Though it takes great effort to amend the Constitution, the process begins with an idea, informed by people's experience, when they see a need for change. We learn some valuable lessons from the Constitution—most importantly that our policies need to be dynamic enough to adjust to changing environments.

The Constitution and the Torah were created from distinct environments, but they both had a similar goal: to serve as rules as well as to guide our behavior and the behavior of those in power. Though our information security policies may not be used for such lofty purposes as the Constitution and the Torah, the need for guidance, direction, and roles remains the same.

Policy Today

We began this chapter with broad examples of the impact of policy throughout history. Let's begin to focus on the organizations for which we will be writing our information security policies—namely, profit, nonprofit and not-for-profit businesses, government agencies, and institutions. The same circumstances that led us to create policies for social culture exist for our corporate culture as well.

Guiding Principles

Corporate culture can be defined as the shared attitudes, values, goals, and practices that characterize a company, corporation, or institution. ***Guiding principles*** set the tone for a corporate culture. Guiding principles synthesize the fundamental philosophy or beliefs of an organization and reflect the kind of company that an organization seeks to be.

FYI: Guiding Principles and Practices

Guiding principles are the fundamental philosophy or beliefs of an organization and the foundation upon which a company is built. Toyota Motor Corporation (TMC) has been a leader in promoting its company vision, guiding principles, values, philosophy, and code of conduct. You can read more about the relationship between Toyota's guiding principles, policies, and everyday practice at www.toyota-global.com/company/toyota_traditions/.

Toyota Guiding Principles[2]

"The Guiding Principles at Toyota (adopted in 1992 and revised in 1997) reflect the kind of company that Toyota seeks to be in light of the unique management philosophy, values, and methods that it has embraced since its foundation. TMC, together with its consolidated subsidiaries, hopes to contribute to sustainable development through its corporate activities based on understanding and sharing of the Guiding Principles at Toyota.

- "Honor the language and spirit of the law of every nation and undertake open and fair business activities to be a good corporate citizen of the world.
- "Respect the culture and customs of every nation and contribute to economic and social development through corporate activities in their respective communities.
- "Dedicate our business to providing clean and safe products and to enhancing the quality of life everywhere through all of our activities.
- "Create and develop advanced technologies and provide outstanding products and services that fulfill the needs of customers worldwide.
- "Foster a corporate culture that enhances both individual creativity and the value of teamwork, while honoring mutual trust and respect between labor and management.
- "Pursue growth through harmony with the global community via innovative management.
- "Work with business partners in research and manufacture to achieve stable, long-term growth and mutual benefits, while keeping ourselves open to new partnerships."

Not all guiding principles and hence corporate cultures are good. As a matter of fact, there are companies for whom greed, exploitation, and contempt are unspoken-yet-powerful guiding principles. You may recall the deadly April 24, 2013 garment factory collapse in Bangladesh where 804 people were confirmed dead and more than 2,500 injured.[3] This is a very sad example of a situation where the lives of many were knowingly put at risk for the sake of making money.

Corporate Culture

Corporate cultures are often classified by how corporations treat their employees and their customers. The three classifications are negative, neutral, and positive. A negative classification is indicative of a hostile, dangerous, or demeaning environment. Workers do not feel comfortable and may not be safe; customers are not valued and may even be cheated. A neutral classification means that the business neither supports nor hinders its employees; customers generally get what they pay for. A positive classification is awarded to businesses that strive to create and sustain a welcoming workplace, truly value the customer relationship, partner with their suppliers, and are responsible members of their community.

Let's consider a tale of two companies. Both companies experience a data breach that exposes customer information; both companies call in experts to help determine what happened. In both cases, the investigators determine that the data-protection safeguards were inadequate and that employees were not properly monitoring the systems. The difference between these two companies is how they respond and learn from the incident. Company A is quick to respond by blaming the department management, firing key employees, and looking for ways to avoid legally required customer notification. Company B leadership shares the report with the department, solicits internal and external feedback on how to improve, researches new controls, methodically implements enhancements, and informs customers in a timely manner so they can take steps to protect themselves.

A positive corporate culture that focuses on protecting internal and customer information, solicits input, engages in proactive education, and allocates resources appropriately makes a strong statement that employees and customers are valued. In these organizations, policy is viewed as an investment and a competitive differentiator for attracting quality employees and customers.

In Practice

The Philosophy of Honoring the Public Trust

Each of us willingly shares a great deal of personal information with organizations that provide us service, and we have an expectation of privacy. Online, we post pictures, profiles, messages, and much more. We disclose and discuss our physical, emotional, mental, and familial issues with health professionals. We provide confidential financial information to accountants, bankers, financial advisors, and tax preparers. The government requires that we provide a myriad data throughout our life, beginning with birth certificates and ending with death certificates. On occasion, we may find ourselves in situations that we must confide in an attorney or clergy. In each of these situations, we expect the information we provide will be protected from unauthorized disclosure, not be intentionally altered, and used only for its intended purpose. We also expect that the systems used to provide the service will be available. The philosophy of honoring the public trust instructs us to be careful stewards of the information with which we have been entrusted. It is the manta of organizations that truly care about those they serve. As you plan your career, consider your potential role in honoring the public trust.

Information Security Policy

The role of policy is to codify guiding principles, shape behavior, provide guidance to those who are tasked with making present and future decisions, and serve as an implementation roadmap. An ***information security policy*** is a directive that defines how the organization is going to protect its information assets and information systems, ensure compliance with legal and regulatory requirements, and maintain an environment that supports the guiding principles. The objective of an information security policy and corresponding program is to protect the organization, its employees, its customers, and also vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information, protect the integrity of the information, and ensure the availability of information systems.

FYI: Information Assets

Information is data with context or meaning. An ***asset*** is a resource with value. As a series of digits, the string 345934353 has no discernible value. However, if those same numbers represented a social security number (345-93-4353) or a bank account number (34-5834353), they would have both meaning and value. ***Information asset*** is the term applied to the information that an organization uses to conduct its business. Examples include customer data, employee records, financial documents, business plans, intellectual property, IT information, reputation, and brand. Information assets may be protected by law or regulation (for example, patient medical history), considered internally confidential (for example, employee reviews and compensation plans), or even publicly available (for example, website content). Information assets are generally stored in digital or print format; however, it is possible to extend our definition to institutional knowledge.

Successful Policy Characteristics

Successful policies establish what must be done and why it must be done, but not how to do it. Good policy has the following seven characteristics:

- **Endorsed**—The policy has the support of management.
- **Relevant**—The policy is applicable to the organization.
- **Realistic**—The policy make sense.
- **Attainable**—The policy can be successfully implemented.
- **Adaptable**—The policy can accommodate change.
- **Enforceable**—The policy is statutory.
- **Inclusive**—The policy scope includes all relevant parties.

Taken together, the characteristics can be thought of as a policy pie, with each slice being equally important, as illustrated in Figure 1.1.

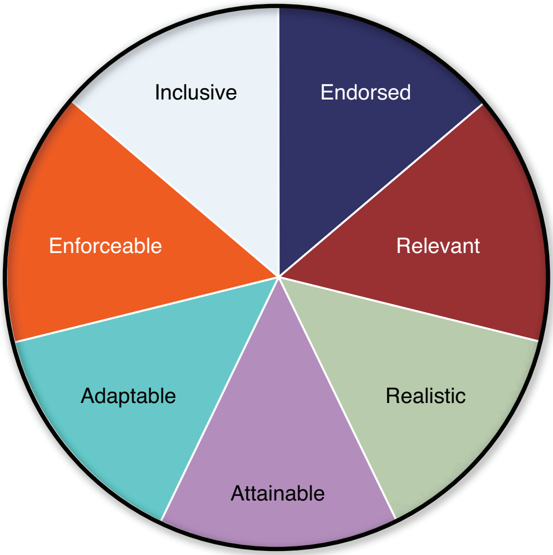


FIGURE 1.1 The policy pie.

Endorsed

We have all heard the saying "Actions speak louder than words." In order for an information security policy to be successful, leadership must not only believe in the policy, they must also act accordingly by demonstrating an active commitment to the policy by serving as role models. This requires visible participation and action, ongoing communication and championing, investment, and prioritization.

Consider this situation: Company A and Company B both decide to purchase iPhones for management and sales personnel. By policy, both organizations require strong, complex email passwords. At both organizations, IT implements the same complex password policy on the iPhone that is used to log in to their webmail application. Company A's CEO is having trouble using the iPhone and he demands that IT reconfigure his phone so he doesn't have to use a password. He states that he is "too important to have to spend the extra time typing in a password, and besides none of his peers have to do so." Company B's CEO participates in rollout training, encourages employees to choose strong passwords in order to protect customer and internal information, and demonstrates to his peers the enhanced security, including a wipe feature after five bad password attempts.

Nothing will doom a policy quicker than having management ignore or, worse, disobey or circumvent it. Conversely, visible leadership and encouragement are two of the strongest motivators known to humankind.

Relevant

Strategically, the information security policy must support the guiding principles and goals of the organization. Tactically, it must be relevant to those who must comply. Introducing a policy to a group of people who find nothing recognizable in relation to their everyday experience is a recipe for disaster.

Consider this situation: Company A's CIO attends a seminar on the importance of physical access security. At the seminar, they distribute a "sample" policy template. Two of the policy requirements are that exterior doors remain locked at all times and that every visitor be credentialed. This may sound reasonable, until you consider that most Company A locations are small offices that require public accessibility. When the policy is distributed, the employees immediately recognize that the CIO does not have a clue about how they operate.

Policy writing is a thoughtful process that must take into account the environment. If policies are not relevant, they will be ignored or, worse, dismissed as unnecessary and management will be perceived as being out of touch.

Realistic

Think back to your childhood to a time you were forced to follow a rule you did not think made any sense. The most famous defense most of us were given by our parents in response to our protests was "Because I said so!" We can all remember how frustrated we became whenever we heard that statement, and how it seemed unjust. We may also remember our desire to deliberately disobey our parents—to rebel against this perceived tyranny. In very much the same way, policies will be rejected if they are not realistic. Policies must reflect the reality of the environment in which they will be implemented.

Consider this situation: Company A discovers that users are writing down their passwords on sticky notes and putting the sticky notes on the underside of their keyboard. This discovery is of concern because multiple users share the same workstation. In response, management decides to implement a policy that prohibits employees from writing down their passwords. Turns out that each employee uses at least six different applications, and each requires a separate login. What's more, on average, the passwords change every 90 days. One can imagine how this policy might be received. More than likely, users will decide that getting their work done is more important than obeying this policy and will continue to write down their passwords, or perhaps they will decide to use the same password for every application. To change this behavior will take more than publishing a policy prohibiting it; leadership needs to understand why employees were writing down their passwords, make employees aware of the dangers of writing down their passwords, and most importantly provide alternative strategies or aids to remember the passwords.

If you engage constituents in policy development, acknowledge challenges, provide appropriate training, and consistently enforce policies, employees will be more likely to accept and follow the policies.

Attainable

Policies should only require what is possible. If we assume that the objective of a policy is to advance the organization's guiding principles, one can also assume that a positive outcome is desired. A policy should never set up constituents for failure; rather, it should provide a clear path for success.

Consider this situation: In order to contain costs and to enhance tracking, Company A's management adopted a procurement policy that purchase orders must be sent electronically to suppliers. They set a goal of 80% electronic fulfillment by the end of the first year and announced that regional offices that do not meet this goal will forfeit their annual bonus. In keeping with existing information security policy, all electronic documents sent externally that include proprietary company information must be sent using the secure file transfer application. The problem is that procurement personnel despise the secure file transfer application because it is slow and difficult to use. Most frustrating of all, it is frequently offline. That leaves them three choices: depend on an unstable system (not a good idea), email the purchase order (in violation of policy), or continue mailing paper-based purchase orders (and lose their bonus).

It is important to seek advice and input from key people in every job role to which the policies apply. If unattainable outcomes are expected, people are set up to fail. This will have a profound effect on morale and will ultimately affect productivity. Know what is possible.

Adaptable

In order to thrive and grow, businesses must be open to changes in the market and willing to take measured risks. A static set-in-stone information security policy is detrimental to innovation. Innovators are hesitant to talk with security, compliance, or risk departments for fear that their ideas will immediately be discounted as contrary to policy or regulatory requirement. "Going around" security is understood as the way to get things done. The unfortunate result is the introduction of products or services that may put the organization at risk.

Consider this situation: Company A and Company B are in a race to get their mobile app to market. Company A's programming manager instructs her team to keep the development process secret and not to involve any other departments, including security and compliance. She has 100% faith in her team and knows that without distractions they can beat Company B to market. Company B's programming manager takes a different tack. She demands that security requirements be defined early in the software development cycle. In doing so, her team identifies a policy roadblock. They have determined that they need to develop custom code for the mobile app but the policy requires that "standard programming languages be used." Working together with the security officer, the programming manager establishes a process to document and test the code in such a way that it meets the intent of the policy. Management agrees to grant an exception and to review the policy in light of new development methodologies.

Company A does get to market first. However, their product is vulnerable to exploit, puts their customers at risk, and ultimately gets bad press. Instead of moving on to the next project, the development team will need to spend their time rewriting code and issuing security updates. Company B gets to market a few months later. They launch a functional, stable, and secure app.

An adaptable information security policy recognizes that information security is not a static, point-in-time endeavor but rather an ongoing process designed to support the organizational mission. The information security program should be designed in such a way that participants are encouraged to challenge conventional wisdom, reassess the current policy requirements, and explore new options without losing sight of the fundamental objective. Organizations that are committed to secure products and services often discover it to be a sales enabler and competitive differentiator.

Enforceable

Enforceable means that administrative, physical, or technical controls can be put in place to support the policy, that compliance can be measured and, if necessary, appropriate sanctions applied.

Consider this scenario: Company A and Company B both have a policy stating that Internet access is restricted to business use only. Company A does not have any controls in place to restrict access; instead, the company leaves it up to the user to determine "business use." Company B implements web-filtering software that restricts access by site category and reviews the filtering log daily. In conjunction with implementing the policy, Company B conducted a training session explaining and demonstrating the rationale for the policy with an emphasis on disrupting the malware delivery channel.

A workstation at Company A is infected with malware. It is determined that the malware came from a website that the workstation user accessed. Company A's management decides to fire the user for "browsing" the web. The user files a protest claiming that the company has no proof that it wasn't business use, that there was no clear understanding of what "business use" meant, and besides everyone (including his manager) is always surfing the web without consequence.

A user at Company B suspects something is wrong when multiple windows start opening while he is at a "business use" website. He immediately reports the suspicious activity. His workstation is immediately quarantined and examined for malware. Company B's management investigates the incident. The logs substantiate the users claim that the access was inadvertent. The user is publicly thanked for reporting the incident.

If a rule is broken and there is no consequence, then the rule is in effect meaningless. However, there must be a fair way to determine if a policy was violated, which includes evaluating the organizational support of the policy. Sanctions should be clearly defined and commensurate with the associated risk. A clear and consistent process should be in place so that all similar violations are treated in the same manner.

Inclusive

It is important to include external parties in our policy thought process. It used to be that organizations only had to be concerned about information and systems housed within their walls. That is no longer the case. Data (and the systems that store, transmit, and process it) are now widely and globally distributed. Organizations that choose to put information in or use systems in "the cloud" may face the additional challenge of having to assess and evaluate vendor controls across distributed systems in multiple locations. The reach of the Internet has facilitated worldwide commerce, which means that policies may have to consider an international audience of customers, business partners, and employees. The trend toward outsourcing and subcontracting requires that policies be designed in such a way to incorporate third parties. Information security policies must also consider external threats such as unauthorized access, vulnerability exploits, intellectual property theft, denial of service attacks, and hacktivism done in the name of cybercrime, terrorism, and warfare.

An information security policy must take into account organizational objectives; international law; the cultural norms of its employees, business partners, suppliers, and customers; environmental impact and global cyber threats. The hallmark of a great information security policy is that it positively affects the organization, its shareholders, employees, and customers, as well as the global community.

FYI: Cyber What?

Coined in 1991, the prefix "cyber"[4] is defined as involving computers or computer networks. Affixed to the terms *crime*, *terrorism*, and *warfare*, cyber means that computer resources or computer networks such as the Internet are used to commit the action.

Richard Clarke, cybersecurity adviser to Presidents Bill Clinton and George W. Bush, in an April 6, 2010 National Public Radio interview with Tom Gjelten, commented that "the difference between cybercrime, cyber-espionage, and cyber-war is a couple of keystrokes. The same technique that gets you in to steal money, patented blueprint information, or chemical formulas is the same technique that a nation-state would use to get in and destroy things."

The Role of Government

In the previous section, we peeked into the world of Company A and Company B and found them to be very different in their approach to information security. In the real world, this is problematic. Information security is complex, and weaknesses in one organization can directly affect another. At times, government intervention is required in order to protect its critical infrastructure and its citizens. Intervention with the purpose of either restraining or causing a specific set of uniform actions is known as ***regulation***. In the 1990s, two groundbreaking pieces of information security–related federal legislation were introduced with the objective of protecting personal financial and medical records:

- The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Modernization Act of 1999, Safeguards Rule
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Gramm-Leach-Bliley Act (GLBA)

On November 12, 1999, President Clinton signed the GLB Act (GLBA) into law. The purpose of the Act was to reform and modernize the banking industry by eliminating existing barriers between banking and commerce. The Act permitted banks to engage in a broad range of activities, including insurance and securities brokering, with new affiliated entities. Lawmakers were concerned that these activities would lead to an aggregation of customer financial information and significantly increase the risk of identity theft and fraud. Section 501B of the legislation, which went into effect May 23, 2003, required that companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance[5] ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. GLBA requires financial institutions and other covered entities to develop and adhere to an information security policy that protects customer information and assigns responsibility for the adherence to the Board of Directors. Enforcement of GLBA was assigned to federal oversight agencies including the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve, the Office of the Comptroller of the Currency (OCC), the National Credit Union Agency (NCUA), and the Federal Trade Commission (FTC).

NOTE

In Chapter 13, "Regulatory Compliance for Financial Institutions," we will examine the regulations applicable to the financial sector, with a focus on the Interagency Guidelines Establishing Information Security Standards, the FTC Safeguards Act, Financial Institutions Letters (FILs), and applicable supplements.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Likewise, the HIPAA Security Rule established a national standard to protect individuals' electronic personal health information (known as ePHI) that is created, received, used, or maintained by a covered entity, which includes healthcare providers and business associates. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Covered entities are required to publish comprehensive information security policies that communicate in detail how information is protected. The legislation, while mandatory, did not include a stringent enforcement process. However, in 2012, one of the provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH) assigned audit and enforcement responsibility to the Department of Health and Human Services Office of Civil Rights (HHS-OCR) and gave state Attorneys General the power to file suit over HIPAA violations in their jurisdiction.

NOTE

In Chapter 14, "Regulatory Compliance for the Healthcare Sector," we will examine the components of the original HIPAA Security Rule, and the subsequent HITECH Act and the Omnibus Rule. We will discuss the policies, procedures, and practices that entities need to implement to be HIPAA-compliant.

In Practice

Protecting Your Student Record

The privacy of your student record is governed by a federal law known as FERPA, which stands for the Family Educational Rights and Privacy Act of 1974. The law states that an educational institution must establish a written institutional policy to protect confidentiality of student education records and that students must be notified of their rights under the legislation. Privacy highlights of the policy include the requirement that schools must have written permission from the parent or eligible students (age 18 and older) in order to release any information from a student's education record. Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them.

States as Leaders

Congress has failed repeatedly to establish a comprehensive national security standard for the protection of digital non-public personally identifiable information (NPPI), including notification of breach or compromise requirements. In the absence of federal legislation, states have taken on the responsibility. On July 1, 2003, California became the first state to enact consumer information security notification legislation. SB 1386: California Security Breach Information Act requires a business or state agency to notify any California resident whose unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person. The law defines personal information as "any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information." Subsequently, 46 states have enacted similar security breach notification laws.

NOTE

In Chapter 11, "Information Security Incident Management," we will discuss the importance of incident response capability and how to comply with the myriad of state data breach notification laws.

On March 1, 2010, Massachusetts became the first state in the nation to require the protection of personally identifiable information of Massachusetts residents. 201 CMR 17: Standards for the Protection of Personal Information of Residents of the Commonwealth establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records and mandates a broad set of safeguards, including security policies, encryption, access control, authentication, risk assessment, security monitoring, and training. Personal information is defined as a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following: social security number, driver's license number or state-issued identification card number, financial account number, or credit or debit card number. The provisions of this regulation apply to all persons who own or license personal information about a resident of the Commonwealth of Massachusetts.

Regulatory compliance is a powerful driver.

In response, untold dollars and workforce hours have been invested in achieving this objective. For some organizations, compliance is the only reason they have an information security policy. Conversely, there are industry sectors that recognize the inherent operational, civic, and reputational benefit of implementing applicable controls and safeguards. Two of the federal regulations mentioned earlier in this chapter—GLBA and HIPAA—were the result of industry and government collaboration. The passage of these regulations forever altered the security landscape. You will learn more about federal and state regulatory requirements and their relationship to information security policies and practices in subsequent chapters.

Information Security Policy Lifecycle

Regardless of whether a policy is based on guiding principles or regulatory requirements, its success depends in large part upon how the organization approaches the tasks of policy development, publication, adoption, and review. Collectively, this process is referred to as the ***policy lifecycle***, as illustrated in Figure 1.2. The responsibilities associated with the policy lifecycle process are distributed throughout an organization as outlined in Table 1.1. Organizations that understand the lifecycle and take a structured approach will have a much better chance of success. The objective of this section is to introduce you to the components that make up the policy lifecycle. Throughout the text, we will examine the process as it relates to specific information security policies.

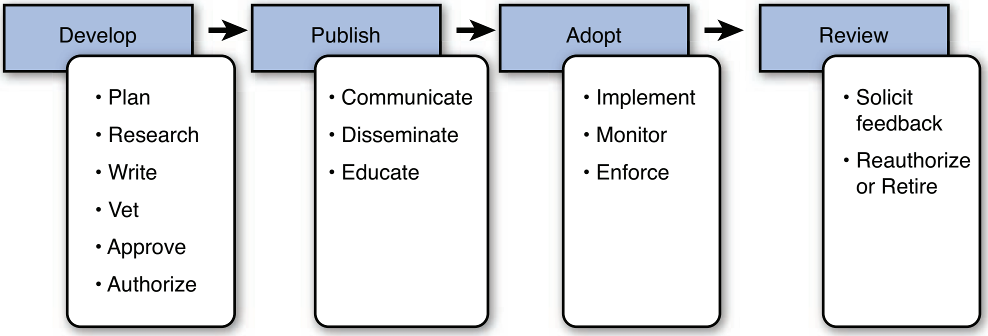


FIGURE 1.2 Information security policy lifecycle.

TABLE 1.1 Information Security Policy Lifecycle Responsibilities

Position	Develop	Publish	Adopt	Review
Board of Directors and/or Executive Management	Communicate guiding principles. Authorize policy.	Champion the policy.	Lead by example.	Reauthorize or approve retirement.
Operational Management	Plan, research, write, vet, and review.	Communicate, disseminate, and educate.	Implement, evaluate, monitor, and enforce.	Provide feedback and make recommendations.
Compliance Officer	Plan, research, contribute, and review.	Communicate, disseminate, and educate.	Evaluate.	Provide feedback and make recommendations.
Auditor			Monitor.	

Policy Development

Even before setting pen to paper, considerable thought and effort need to be put into developing a policy. Once the policy is written, it still needs to go through an extensive review and approval process. There are six key tasks in the development phase: planning, researching, writing, vetting, approving, and authorizing.

1. The seminal ***planning*** task should identify the need for and context of the policy. Policies should never be developed for their own sake. There should always be a reason. Polices may be needed to support business objectives, contractual obligations, or regulatory requirements. The context could vary from the entire organization to a specific subset of users. In Chapters 4 through 12, we will identify the reasons for specific policies.

2. Policies should support and be in agreement with relevant laws, obligations, and customs. The ***research*** task focuses on defining operational, legal, regulatory, or contractual requirements and aligning the policy with the aforementioned. This objective may sound simple, but in reality is extremely complex. Some regulations and contracts have very specific requirements whereas others are extraordinarily vague. Even worse, they may contradict each other.

   For example, federal regulation requires financial institutions to notify consumers if their account information has been compromised. The notification is required to include details about the breach; however, Massachusetts Law 201 CMR 17:00: Standards for the Protection of Personal Information of Residents of the Commonwealth specifically restricts the same details from being included in the notification. You can imagine the difficult in trying to comply with opposing requirements. Throughout this text, we will align policies with legal requirements and contractual obligations.

3. In order to be effective, policies must be written for their intended audience. Language is powerful and is arguably one of the most important factors in gaining acceptance and, ultimately, successful implementation. The ***writing*** task requires that the audience is identified

and understood. In Chapter 2, “Policy Elements and Style,” we will explore the impact of the plain writing movement on policy development.

4. Policies require scrutiny. The ***vetting*** task requires the authors to consult with internal and external experts, including legal counsel, human resources, compliance, information security and technology professionals, auditors, and regulators.

5. Because information security policies affect an entire organization, they are inherently cross-departmental. The ***approval*** task requires that the authors build consensus and support. All affected departments should have the opportunity to contribute to, review, and, if necessary, challenge the policy before it is authorized. Within each department, key people should be identified, sought out, and included in the process. Involving them will contribute to the inclusiveness of the policy and, more importantly, may provide the incentive for them to champion the policy.

6. The ***authorization*** task requires that executive management or an equivalent authoritative body agree to the policy. Generally, the authority has oversight responsibilities and can be held legally liable. Both GLBA and HIPAA require written information security policies that are Board-approved and subject to at least annual review. Boards of Directors are often composed of experienced albeit nontechnical business people from a spectrum of industry sectors. It is helpful to know who the Board members are, and their level of understanding, so that policies are presented in a meaningful way.

Policy Publication

Once you have the “green light” from the authority, it is time to publish and introduce the policy to the organization as a whole. This introduction will require careful planning and execution because it will set the stage for how well the policy is accepted and followed. There are three key tasks in the publication phase: communication, dissemination, and education.

1. The objective of the ***communication*** task is to deliver the message that the policy or policies are important to the organization. In order to accomplish this task, visible leadership is required. There are two very distinct types of leaders in the world: those who see leadership as a responsibility and those who see it as a privilege.

   Leaders who see their role as a responsibility adhere to all the same rules they ask others to follow. “Do as I do” is an effective leadership style, especially in relation to information security. Security is not always convenient, and it is crucial for leadership to participate in the information security program by adhering to its policies and setting the example.

   Leaders who see their role as a privilege have a powerful negative impact: “Do as I say, not as I do.” This leadership style will do more to undermine an information security program than any other single force. As soon as people learn that leadership is not subject to the same rules and restrictions, policy compliance and acceptance will begin to erode.

Invariably, the organizations in which leadership sets the example by accepting and complying with their own policy have fewer information security–related incidents. When incidents do occur, they are far less likely to cause substantial damage. When the leadership sets a tone of compliance, the rest of the organization feels better about following the rules, and they are more active in participating. In Chapter 4, "Governance and Risk Management," we will examine the relationship between governance and security.

2. ***Disseminating*** the policy simply means making it available. Although the task seems obvious, it is mind boggling how many organizations store their policies in locations that make them, at best, difficult to locate and, at worst, totally inaccessible. Policies should be widely distributed and available to their intended audience. This does not mean that all polices should be available to everyone because there may be times when certain polices contain confidential information that should only be made available on a restricted or need-to-know basis.

3. Companywide training and ***education*** build culture. When people share experiences, they are drawn together; they can reinforce one another's understanding of the subject matter and therefore support whatever initiative the training was intended to introduce. Introducing information security policies should be thought of as a teaching opportunity with the goal of raising awareness, and giving each person a tangible connection to the policy objective. Initial education should be coupled with ongoing awareness programs designed to reinforce the importance of policy-driven security practices.

   Multiple factors contribute to an individual's decision to comply with a rule, policy, or law, including the chance of being caught, the reward for taking the risk, and the consequences. Organizations can influence individual decision making by creating direct links between individual actions, policy, and success. Creating a ***culture of compliance*** means that each participant not only recognizes and understands the purpose of a policy, they also actively look for ways to champion the policy. ***Championing*** a policy means being willing to demonstrate visible leadership and to encourage and educate others. Creating a culture of information security policy compliance requires an ongoing investment in training and education, measurements, and feedback.

NOTE

In Chapter 6, "Human Resources Security," we will examine the National Institute of Standards and Technology (NIST) Security Awareness, Training, and Education (SETA) model.

Policy Adoption

The policy has been announced and the reasons communicated. Now the hard work of adoption starts. Successful adoption begins with an announcement, progresses through implementation, performance evaluation, and process improvement, with the ultimate goal being normative integration. For our purposes, ***normative integration*** means that the policy and corresponding implementation is expected behavior—all others being deviant. There are three key tasks in the adoption phase: implementation, monitoring, and enforcement:

1. ***Implementation*** is the busiest and most challenging task of all. The starting point is ensuring that everyone involved understands the intent of the policy as well as how it is to be applied. Decisions may need to be made regarding the purchase and configuration of supporting administrative, physical, and technical controls. Capital investments may be need to be budgeted for. A project plan may need to be developed and resources assigned. Management and affected personnel need to be kept informed. Situations where implementation is not possible need to be managed, including a process for granting either temporary or permanent exceptions.

2. Post-implementation, compliance and policy effectiveness need to be ***monitored*** and reported. Mechanisms to monitor compliance range from application-generated metrics to manual audits, surveys, and interviews as well as violation and incident reports.

3. Unless there is an approved exception, policies must be ***enforced*** consistently and uniformly. The same is true of violation consequences. If a policy is enforced only for certain circumstances and people, or if enforcement depends on which supervisor or manager is in charge, eventually there will be adverse consequences. Once there is talk within an organization that different standards for enforcement exist, the organization is open to many cultural problems, the most severe of which involve discrimination lawsuits.

Policy Review

Change is inherent in every organization. Policies must support the guiding principles, organizational goals, and forward-facing initiatives. They must also be harmonized with regulatory requirements and contractual obligations. The two key tasks in the review phase are soliciting feedback and reauthorizing or retiring policies:

1. Continuing acceptance of information security policies hinges on making sure the policies keep up with significant changes in the organization or the technology infrastructure. Policies should be reviewed annually. Similar to the development phase, feedback should be ***solicited*** from internal and external sources.

2. Policies that are outdated should be refreshed. Policies that are no longer applicable should be retired. Both tasks are important to the overall perception of the importance and applicability of organizational directives. The outcome of the annual review should either be policy ***reauthorization*** or policy ***retirement***. The final determination belongs with the Board of Directors or equivalent body.

Summary

In this chapter, we discussed the various roles policies play, and have played, in many forms of social structures—from entire cultures to corporations. You learned that policies are not new in the world. When its religious intent is laid aside, the Torah reads like any other secular code of law or policy. The people of that time were in desperate need of guidance in their everyday existence to bring order to their society. You learned that policies give us a way to address common foreseeable situations and guide us to make decisions when faced with them. Similar to the circumstances that brought forth the Torah 3,000 years ago, our country found itself in need of a definite structure to bring to life the ideals of our founders, and to make sure those ideals remained intact. The U.S. Constitution was written to fulfill that purpose and serves as an excellent example of a strong, flexible, and resilient policy document.

We applied our knowledge of historical policy to the present day, examining the role of corporate culture, specifically as it applies to information security policy. Be it societal, government, or corporate, policy codifies guiding principles, shapes behavior, provides guidance to those who are tasked with making present and future decisions, and serves as an implementation roadmap. Because not all organizations are motivated to do the right thing and because weaknesses in one organization can directly affect another, there are times when government intervention is required. We considered the role of government policy—specifically the influence of groundbreaking federal and state legislation related to the protection of NPPI in the public and privacy sectors.

The objective of an information security policy is to protect the organization, its employees, its customers, and also its vendors and partners from harm resulting from intentional or accidental damage, misuse, or disclosure of information, as well as to protect the integrity of the information and ensure the availability of information systems. We examined in depth the seven common characteristics of a successful information security policy as well as the policy lifecycle. The seven common characteristics are endorsed, relevant, realistic, attainable, adaptable, enforceable, and inclusive. The policy lifecycle spans four phases: develop, publish, adopt, and review. Policies need champions. Championing a policy means being willing to demonstrate visible leadership and to encourage and educate others with the objective of creating a culture of compliance, where participants not only recognize and understand the purpose of a policy, they also actively look for ways to promote it. The ultimate goal is normative integration, meaning that the policy and corresponding implementation is the expected behavior, all others being deviant.

Throughout the text, we build on these fundamental concepts. In Chapter 2, you will learn the discrete components of a policy and companion documents as well as the technique of plain writing.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Policies define which of the following?

   A. Rules
   B. Expectations
   C. Patterns of behavior
   D. All of the above

2. Without policy, human beings would live in a state of _______.

   A. chaos
   B. bliss
   C. harmony
   D. laziness

3. A guiding principle is best described as which of the following?

   A. A financial target
   B. A fundamental philosophy or belief
   C. A regulatory requirement
   D. A person in charge

4. Which of the following best describes corporate culture?

   A. Shared attitudes, values, and goals
   B. Multiculturalism
   C. A requirement to all act the same
   D. A religion

5. Which of the following is a true statement?

   A. Corporate culture is the same as policy.
   B. Guiding principles set the tone for a corporate culture.
   C. All corporate cultures are positive.
   D. Guiding principles should be kept secret.

6. Which of the following best describes the role of policy?

   A. To codify guiding principles

   B. To shape behavior

   C. To serve as a roadmap

   D. All of the above

7. An information security policy is a directive that defines which of the following?

   A. How employees should do their jobs

   B. How to pass an annual audit

   C. How an organization protects information assets and systems

   D. How much security insurance a company should have

8. Which of the following is not an example of an information asset?

   A. Customer financial records

   B. Marketing plan

   C. Patient medical history

   D. Building graffiti

9. What are the seven characteristics of a successful policy?

   A. Endorsed, relevant, realistic, cost-effective, adaptable, enforceable, inclusive

   B. Endorsed, relevant, realistic, attainable, adaptable, enforceable, inclusive

   C. Endorsed, relevant, realistic, technical, adaptable, enforceable, inclusive

   D. Endorsed, relevant, realistic, legal, adaptable, enforceable, inclusive

10. A policy that has been endorsed has the support of which of the following?

    A. Customers

    B. Creditors

    C. The union

    D. Management

11. Who should always be exempt from policy requirements?

    A. Employees

    B. Executives

    C. No one

    D. Salespeople

12. “Attainable” means that the policy ___________.

    A. can be successfully implemented

    B. is expensive

    C. only applies to suppliers

    D. must be modified annually

13. Which of the following statements is always true?

    A. Policies stifle innovation.

    B. Policies make innovation more expensive.

    C. Policies should be adaptable.

    D. Effective policies never change.

14. If a policy is violated and there is no consequence, the policy is considered to be which of the following?

    A. Meaningless

    B. Inclusive

    C. Legal

    D. Expired

15. Who must approve the retirement of a policy?

    A. A compliance officer

    B. An auditor

    C. Executive management or the Board of Directors

    D. Legal counsel

16. Which of the following sectors is not considered part of the “critical infrastructure”?

    A. Public health

    B. Commerce

    C. Banking

    D. Chemical industry

17. Which term best describes government intervention with the purpose of causing a specific set of actions?

    A. Deregulation

    B. Politics

    C. Regulation

    D. Amendments

18. The objectives of GLBA and HIPAA, respectively, are to protect __________.

- **A.** financial and medical records
- **B.** financial and credit card records
- **C.** medical and student records
- **D.** judicial and medical records

19. Which of the following states was the first to enact consumer breach notification?

- **A.** Kentucky
- **B.** Colorado
- **C.** Connecticut
- **D.** California

20. In 2010, Massachusetts became the first state in the nation to require _________.

- **A.** minimum standards for the protection of personally identifiable information of non-residents
- **B.** minimum standards for the protection of personally identifiable information of Massachusetts residents
- **C.** maximum standards for the protection of personally identifiable information of Massachusetts residents
- **D.** consumer notification of a breach

21. Which of the following terms best describes the process of developing, publishing, adopting, and reviewing a policy?

- **A.** Policy two-step
- **B.** Policy aging
- **C.** Policy retirement
- **D.** Policy lifecycle

22. Who should be involved in the process of developing policies?

- **A.** Only upper-management-level executives
- **B.** Only part-time employees
- **C.** Personnel throughout the company
- **D.** Only outside, third-party consultants

23. Which of the following does *not* happen in the policy development phase?

- **A.** Planning
- **B.** Enforcement
- **C.** Authorization
- **D.** Approval

24. Which of the following occurs in the policy publication phase?

- **A.** Communication
- **B.** Policy dissemination
- **C.** Education
- **D.** All of the above

25. Normative integration is the goal of the adoption phase. This means ________.

- **A.** Ahere are no exceptions to the policy.
- **B.** The policy passes the stress test.
- **C.** The policy becomes expected behavior, all others being deviant.
- **D.** The policy costs little to implement.

26. How often should policies be reviewed?

- **A.** Never
- **B.** Only when there is a significant change
- **C.** Annually
- **D.** At least annually or sooner if there is a significant change

27. Which of the following phrases best describes the concept of "championing a policy"?

- **A.** A willingness to lead by example, encourage, and educate
- **B.** Winning a compliance award
- **C.** Voting to authorize a policy
- **D.** None of the above

28. Which of the following phrases best describes the philosophy of "honoring the public trust"?

- **A.** Being respectful of law enforcement
- **B.** Contributing to political campaigns
- **C.** Being a careful steward of information in your care
- **D.** Visiting government monuments

29. Who should authorize policies?

    A. Directors or executive management

    B. Operational managers

    C. Employees

    D. Legal counsel

30. Which of the following statements is *not* an objective of information security?

    A. To protect information and information systems from intentional misuse

    B. To protect information and information systems from compromise

    C. To protect information and information systems from destruction

    D. To protect information and information systems from authorized users

EXERCISES

EXERCISE 1.1: Understanding Guiding Principles

1. Reread the sidebar titled "FYI: Guiding Principles and Practices" in this chapter.
2. Choose one of the listed guiding principles at Toyota and describe how a car company could achieve that objective.

EXERCISE 1.2: Identifying Corporate Culture

1. Identify a shared attitude, value, goal, or practice that characterizes the culture of your school or workplace.
2. Describe how you first became aware of the campus or workplace culture.

EXERCISE 1.3: Understanding the Impact of Policy

1. Either at school or workplace, identify a policy that in some way affects you. For example, examine a grading policy or an attendance policy.
2. Describe how the policy benefits (or hurts) you.
3. Describe how the policy is enforced.

EXERCISE 1.4: Understanding Critical Infrastructure

1. Reread the "FYI: National Security" sidebar presented at the beginning of this chapter.
2. Explain what is meant by "critical infrastructure."
3. What concept was introduced in Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience (2013) and why is this important?

EXERCISE 1.5: Understanding Cyber Threats

1. What is the difference between cybercrime, cyber-espionage, and cyber-warfare?
2. What are the similarities?
3. Are cyber threats escalating or diminishing?

PROJECTS

PROJECT 1.1: Honoring the Public Trust

1. Banks and credit unions are entrusted with personal financial information. By visiting financial institution websites, find an example of a policy or practice that relates to protecting customer information or privacy.
2. Hospitals are entrusted with personal health information. By visiting hospital websites, find an example of a policy or practice that relates to protecting patient information or privacy.
3. In what ways are the policies or practices of banks similar to those of hospitals? How are they different?
4. Do either the bank policies or the hospital policies reference applicable regulatory requirements (for example, GLBA or HIPAA)?

PROJECT 1.2: Understanding Government Policy

The passage of the Affordable Care Act requires all U.S. citizens and lawful residents to have health insurance or pay a penalty. This requirement is a government policy.

1. The hallmark of a good policy is that it is endorsed, relevant, realistic, attainable, adaptable, enforceable, and inclusive. Choose four of these characteristics and apply it to the health insurance requirement. Explain why or why not the policy meets the criteria.
2. Policies must be championed. Find an example of a person or group who championed this requirement. Explain how they communicated their support.

PROJECT 1.3: Developing Communication and Training Skills

You have been tasked with introducing a new security policy to your campus. The new policy requires that all students and employees wear identification badges with their name and picture and that guests be given visitor badges.

1. Explain why an institution would adopt this type of policy.
2. Develop a strategy to communicate this policy campus-wide.
3. Design a five-minute training session introducing the new policy. Your session must include participant contribution and a five-question, post-session quiz to determine if the training was effective.

Case Study

The Tale of Two Credit Unions

Best Credit Union members really love doing business with the credit union. The staff is friendly, the service is top notch, and the entire team is always pitching in to help the community. The credit union's commitment to honoring the public trust is evident in its dedication to security best practices. New employees are introduced to the information security policy during orientation. Everyone participates in annual information security training.

The credit union across town, OK Credit Union, doesn't have the same reputation. When you walk in the branch, it is sometimes hard to get a teller's attention. Calling is not much better, as you may find yourself on hold for a long time. Even worse, it is not unusual to overhear an OK Credit Union employee talking about a member in public. OK Credit Union does not have an information security policy. It has never conducted any information security or privacy training.

Best Credit Union wants to expand its presence in the community so it acquires OK Credit Union. Each institution will operate under its own name. The management team at Best Credit Union will manage both institutions.

You are the Information Security Officer at Best Credit Union. You are responsible for managing the process of developing, publishing, and adopting an information security policy specifically for OK Credit Union. The CEO has asked you to write up an action plan and present it at the upcoming management meeting.

Your action plan should include the following:

- What you see as the biggest obstacle or challenge to accomplishing this task
- Which other personnel at Best Credit Union should be involved in this project and why
- Who at OK Credit Union should be invited to participate in the process and why
- How are you going to build support for the process and ultimately for the policy
- What happens if OK Credit Union employees start grumbling about "change"
- What happens if OK Credit Union employees do not or will not comply with the new information security policy

References

1. "What Is Critical Infrastructure?" official website of the Department of Homeland Security, accessed 05/06/2013, http://www.dhs.gov/what-critical-infrastructure.
2. "Guiding Principles at Toyota," official website of Toyota, accessed 05/10/2013, http://www.toyota-global.com/company/vision_philosophy/guiding_principles.html.
3. "Bangladesh building collapse death toll over 800," *BBC News Asia*, accessed 05/08/2013, http://www.bbc.co.uk/news/world-asia-22450419.

4. "Cyber," *Merriam-Webster Online*, accessed 05/09/2013, http://www.merriam-webster.com/dictionary/cyber.

5. "Gramm-Leach-Bliley Act," Federal Trade Commission, Bureau of Consumer Protection Business Center, accessed 05/08/2013, http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

Regulations and Directives Cited

"Presidential Policy Directive—Critical Infrastructure Security and Resilience," official website of the White House, accessed 05/06/2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

"Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," official website of the Department of Homeland Security, accessed 05/06/2013, http://www.dhs.gov/homeland-security-presidential-directive-7#1.

"16 CFR Part 314 Standards for Safeguarding Customer Information: Final Rule," Federal Register, accessed 05/06/2013, http://ithandbook.ffiec.gov/media/resources/3337/joisafeguard_customer_info_final_rule.pdf.

"The Security Rule (HIPAA)," official website of the Department of Health and Human Services, accessed 05/06/2013, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

"State of California SB 1386: California Security Breach Information Act, CIVIL CODE SECTION 1798.80-1798.84," official California legislative information, accessed 05/06/2013, http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84.

"201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH," official website of the Office of Consumer Affairs & Business Regulation (OCABR), accessed 05/06/2013, http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

"Family Educational Rights and Privacy Act (FERPA)," official website of the U.S. Department of Education, accessed 05/10/2013, http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

Other References

Guel, Michele. “A Short Primer for Developing Security Policies,” SANS Institute, accessed 05/02/2012, http://www.sans.org/securityresources/policies/Policy_Primer.pdf.

Krause, Micki, CISSP, and Harold F. Tipton, CISSP. *Information Security Management Handbook, Fifth Edition*. Boca Raton, Florida: CRC Press, Auerbach Publications, 2004.

Chapter 2

Policy Elements and Style

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Distinguish between a policy, a standard, a procedure, a guideline, and a plan.
- Identify policy elements.
- Include the proper information in each element of a policy.
- Know how to use “plain language.”

In Chapter 1, “Understanding Policy,” you learned that policies have played a significant role in helping us form and sustain our social, governmental, and corporate organizations. In this chapter, we begin by examining the hierarchy and purpose of guiding principles, policy, standards, procedures, and guidelines as well as adjunct plans and programs. Returning to our focus on policies, we examine the standard components and composition of a policy document. You will learn that even a well-constructed policy is useless if it doesn’t deliver the intended message. The end result of complex, ambiguous, or bloated policy is, at best, noncompliance. At worst, it leads to disastrous consequences. In this chapter, you will be introduced to “plain language,” which means using the simplest, most straightforward way to express an idea. Plain-language documents are easy to read, understand, and act on. By the end of the chapter, you will have the skills to construct policy and companion documents.

Policy Hierarchy

As you learned in Chapter 1, a policy is a mandatory governance statement that presents management’s position. A well-written policy clearly defines guiding principles, provides guidance to those who must make present and future decisions, and serves as an implementation roadmap. Policies are important, but alone they are limited in what they can accomplish. Policies need supporting documents to give them context and meaningful application. Standards, baselines, guidelines, and procedures each play a significant role in ensuring implementation of the governance objective. The relationship between the documents is known as the ***policy hierarchy***. In a hierarchy, with the exception of the topmost object, all objects are subordinate to the one above it. In a policy hierarchy, the topmost object is the guiding principles, as illustrated in Figure 2.1.

Polices reflect the guiding principles and organizational objectives. Standards enable the policies by defining action. Guidelines, procedures, and baselines support the standards. Let's take a closer look at each of these concepts.

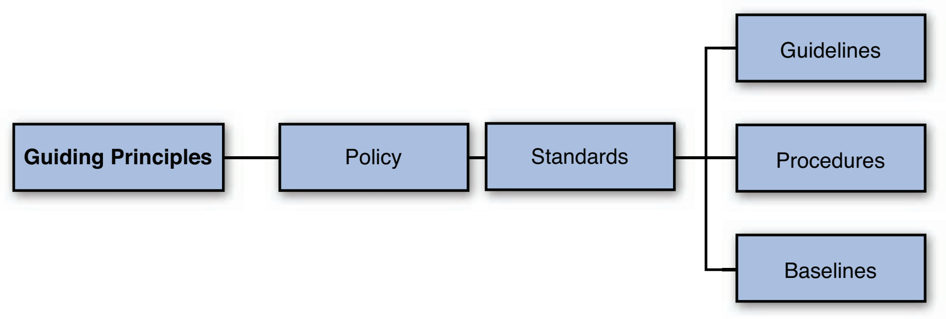


FIGURE 2.1 Policy hierarchy.

Standards

Standards serve as specifications for the implementation of policy and dictate mandatory requirements. For example, our password policy might simply state the following:

1. All users must have a unique user ID and password that conforms to the company password standard.
2. Users must not share their password with anyone regardless of title or position.
3. If a password is suspected to be compromised, it must be reported immediately to the help desk and a new password must be requested.

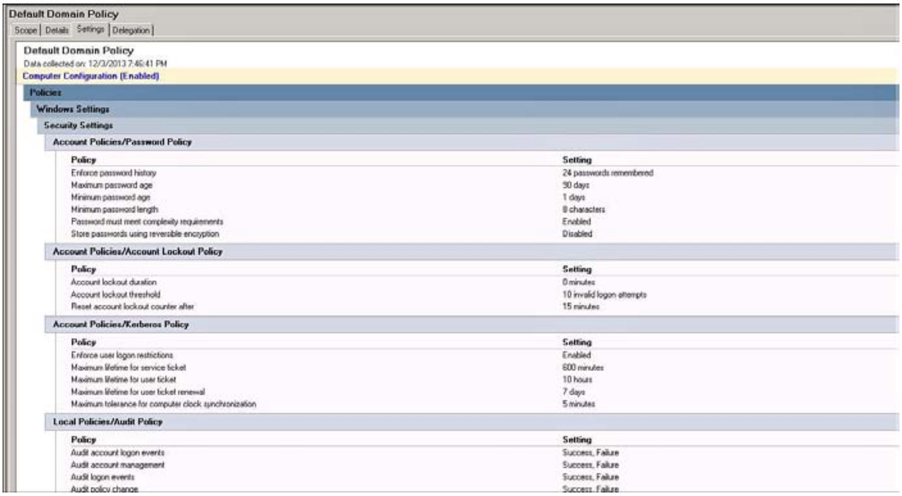
The password standard would then dictate the required password characteristics, such as the following:

- Minimum of eight upper- and lowercase alphanumeric characters
- Must include at least one special character (such as *, &, $, #, !, or @)
- Must not include the user's name, the company name, or office location
- Must not include repeating characters (for example, 111)

As you can see, the policy represents expectations that are not necessarily subject to changes in technology, processes, or management. The standard, however, is very specific to the infrastructure. Standards are determined by management, and unlike policies, they are not subject to Board of Directors authorization. Standards can be changed by management as long as they conform to the intent of the policy.

Baselines

Baselines are an aggregate of implementation standards and security controls for a specific category or grouping, such as platform (for example, Windows OS), device type (for example, iPad), ownership (for example, employee owned), and location (for example, mobile users). The primary objective of a baseline is uniformity and consistency. An example of a baseline related to our password policy and standard example is the mandate that a specific Active Directory Group Policy configuration be used on all Windows devices to technically enforce security requirements, as illustrated in Figure 2.2.



Default Domain Policy

Default Domain Policy
Data collected on: 12/3/2013 7:46:41 PM
Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	0 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit policy change	Success, Failure

FIGURE 2.2 Windows Group Policy settings.

In this example, by applying the same Active Directory Group Policy to all Windows workstations and servers, the standard was implemented throughout the organization. In this case, there is also assurance that new devices will be configured accordingly.

Guidelines

Guidelines are best thought of as teaching tools. The objective of a guideline is to help people conform to a standard. In addition to using softer language than standards, guidelines are customized for the intended audience and are not mandatory. Guidelines are akin to suggestions or advice. A guideline related to the password standard in the previous example might read like this:

"A good way to create a strong password is to think of a phrase, song title, or other group of words that is easy to remember and then convert it, like this:

- "The phrase 'Up and at 'em at 7!' can be converted into a strong password such as **up&atm@7!**.
- "You can create many passwords from this one phrase by changing the number, moving the symbols, or changing the punctuation mark."

This guideline is intended to help readers create easy-to-remember, yet strong passwords.

Procedures

Procedures are instructions for how a policy, standard, baseline, and guidelines are carried out in a given situation. Procedures focus on actions or steps, with a specific starting and ending point. There are four commonly used procedure formats:

- **Simple Step**—Lists sequential actions. There is no decision making.
- **Hierarchical**—Includes both generalized instructions for experienced users and detailed instructions for novices.
- **Graphic**—This format uses either pictures or symbols to illustrate the step.
- **Flowchart**—Used when a decision-making process associated is with the task.

In keeping with our previous password example, let's take a look at a Simple Step procedure for changing a user's Windows password:

1. Press and hold the Ctrl+Alt+Delete keys.
2. Click the Change Password option.
3. Type your current password in the top box.
4. Type your new password in both the second and third boxes. (If the passwords don't match, you will be prompted to reenter your new password.)
5. Click OK and then log in with your new password.

NOTE

As with guidelines, it is important to know both your audience and the complexity of the task when designing procedures. In Chapter 8, "Communications and Operations Security," we discuss in detail the use of standard operating procedures (SOPs).

Plans and Programs

The function of a plan is to provide strategic and tactical instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain timeframe, usually with defined stages and with designated resources. Plans are sometimes referred to as programs. For our purposes, the terms are interchangeable. Here are some examples of information security–related plans we discuss in this book:

- Vendor Management Plan
- Incident Response Plan
- Business Continuity Plan
- Disaster Recovery Plan

Policies and plans are closely related. For example, an Incident Response Policy will generally include the requirement to publish, maintain, and test an Incident Response Plan. Conversely, the Incident Response Plan gets its authority from the policy. Quite often, the policy will be included in the plan document.

In Practice

Policy Hierarchy Review

Let's look at an example of how standards, guidelines, and procedures support a policy statement:

- The standard specifies the type of encryption that must be used.
- The guideline might illustrate how to identify removable media.
- The procedure would provide the instructions for encrypting the media.

Policy Format

Writing policy documents can be challenging. Polices are complex documents that must be written to withstand legal and regulatory scrutiny while at the same time be easily read and understood by the reader. The starting point for choosing a format is identifying the policy audience.

Policy Audience

Who the policy is intended for is referred to as the ***policy audience***. It is imperative, during the planning portion of the security policy project, to clearly define the audience. Policies may be intended for a particular group of employees based on job function or role. An application development policy is targeted to developers. Other policies may be intended for a particular group or individual based on organizational role, such as a policy defining the responsibility of the Information Security Officer. The policy, or portions of it, can sometimes apply to people outside of the company, such as business partners, service providers, contractors, or consultants. The policy audience is a potential resource during the entire policy lifecycle. Indeed, who better to help create and maintain an effective policy than the very people whose job it is to use those policies in the context of their everyday work?

Policy Format Types

Organize, before you begin writing! It is important to decide how many sections and subsections you will require before you put pen to paper. Designing a template that allows the flexibility of editing will save considerable time and reduce aggravation.

There are two schools of thought in regard to policy format. The first is to write each policy as a discrete document; this document type is referred to as a singular policy. The second is to group like policies together; this document type is referred to as a consolidated policy. Consolidated policies are often organized by section and subsection. Table 2.1 illustrates policy document format options.

TABLE 2.1 Policy Document Format Options

Description	Example
Singular policy	Information Security Officer Policy: Specific to the role and responsibility of the Information Security Officer.
Consolidated policy section	Governance Policy: Addresses the role and responsibilities of the Board of Directors, executive management, Chief Risk Officer, Information Security Officer, Compliance Officer, legal counsel, auditor, IT Director, and users.

The advantage to individual policies is that each policy document can be short, clean and crisp, and targeted to its intended audience. The disadvantage is the need to manage multiple policy documents and the chance that they will become fragmented and lose consistency. The advantage to consolidation is that it presents a composite management statement in a single voice. The disadvantage is the potential size of the document and the reader challenge of locating applicable sections.

In the first edition of this book, we limited our study to singular documents. Since then, both the use of technology and the regulatory landscape have increased exponentially—only outpaced by escalating threats. In response to this ever-changing environment, the need for and number of policies has grown. For many organizations, managing singular policies has become unwieldy. The current trend is toward consolidation. Throughout this edition, we are going to be consolidating policies by security domain. You will be introduced to each security domain in Part II, "Information Security Policy Domains."

Regardless of which format you choose, do not include standards, baselines, guidelines, or procedures in your policy document. If you do so, you will end up with one big unruly document. You will undoubtedly encounter one or more of the following problems:

- **Management challenge**—Who is responsible for managing and maintaining a document that has multiple contributors?
- **Difficulty of updating**—Because standards, guidelines, and procedures change far more often than policies, updating this whale of a document will be far more difficult than if these elements were properly treated separately. Version control will become a nightmare.
- **Cumbersome approval process**—Various regulations as well as the Corporate Operating Agreement require that the Board of Directors approve new policies as well as changes. Mashing it all together means that every change to a procedure, guideline, or standard will potentially require the Board to review and approve. This will become very costly and cumbersome for everyone involved.

Policy Components

Policy documents have multiple sections or components (see Table 2.2). How the components are used and in what order will depend on which format—singular or consolidated—you choose. In this section, we examine the composition of each component. Consolidated policy examples are provided in the "In Practice" sidebars.

TABLE 2.2 Policy Document Components

Component	Purpose
Version control	To track changes
Introduction	To frame the document
Policy heading	To identify the topic
Policy goals and objectives	To convey intent
Policy statement	Mandatory directive
Policy exceptions	To acknowledge exclusions
Policy enforcement clause	Violation sanctions
Administrative notations	Additional information
Policy definitions	Glossary of terms

Version Control

Best practices dictate that policies are reviewed annually to ensure they are still applicable and accurate. Of course, policies can (and should) be updated whenever there is a relevant change driver. Version control, as it relates to policies, is the management of changes to the document. Versions are usually identified by a number or letter code. Major revisions generally advance to the next letter or digit (for example, from 2.0 to 3.0). Minor revisions generally advance as a subsection (for example, from 2.0 to 2.1). Version control documentation should include the change date, name of the person or persons making the change, a brief synopsis of the change, the name of the person, committee, or board that authorized the change, and the effective date of the change.

- For singular policy documents, this information is split between the policy heading and the administrative notation sections.
- For consolidated policy documents, a version control table is included either at the beginning of the document or at the beginning of a section.

In Practice

Version Control Table

Version control tables are used in consolidated policy documents. The table is located after the title page, before the table of contents. Version control provides the reader with a history of the document. Here's an example:

V.	Editor	Purpose	Change Description	Authorized By	Effective Date
1.0	S. Ford, EVP		Original.	Sr. management committee	01/17/11
1.1	S. Ford, EVP	Subsection addition	2.5: Disclosures to Third Parties.	Sr. management committee	03/07/11
1.2	S. Ford, EVP	Subsection update	4.4: Border Device Management. 5.8: Wireless Networks.	Sr. management committee	01/14/12
--	S. Ford, EVP	Annual review	No change.	Sr. management committee	01/18/13
2.0	B. Lin, CIO	Section revision	Revised “Section 1.0: Governance and Risk Management” to reflect internal reorganization of roles and responsibilities.	Acme, Board of Directors	05/13/13

Introduction

Think of the introduction as the opening act. This is where we first meet the reader and have the opportunity to engage them. Here are the objectives of the introduction:

- To provide context and meaning
- To convey the importance of understanding and adhering to the policy

- To acquaint the reader with the document and its contents
- To explain the exemption process as well as the consequence of noncompliance
- To thank the reader and to reinforce the authority of the policy

The first part of the introduction should make the case for why policies are necessary. It is a reflection of the guiding principles, defining for the reader the core values the company believes in and is committed to. This is also the place to set forth the regulatory and contractual obligations that the company has—often by listing which regulations, such as GLBA, HIPAA, or MA CMR 17 201, pertain to the organization as well as the scope of the policy.

The second part of the introduction should leave no doubt that compliance is mandatory. A strong statement of expectation from a senior authority such as the Chairman of the Board, CEO, or President is appropriate. Readers should understand that they are unequivocally and directly responsible for the safeguarding of information and systems in the course of their normal employment or relationship with the company. It should also make clear that questions are welcome and a resource is available who can clarify the policy and/or assist with compliance.

The third part of the introduction should describe the policy document, including the structure, categories, and storage location (for example, the company intranet). It should also reference companion documents such as standards, guidelines, programs, and plans.

The fourth part of the introduction should explain how to handle situations where compliance may not be feasible. It should explain the exemption process. The section should also address the consequences of willful noncompliance.

The introduction should end with a “thank you” and with words of encouragement. The introduction should be signed by a person who has the authority to enforce the policy. This final statement reinforces the organizational commitment.

- For singular policy documents, the introduction should be a separate document.
- For consolidated policy documents, the introduction serves as the preface and follows the version control table.

In Practice

Introduction

The introduction has five objectives: to provide context and meaning, to convey the importance of understanding and adhering to the policy, to acquaint the reader with the document, to explain the exemption process and the consequence of noncompliance, and lastly to thank the reader and reinforce the authority of the policy. Each objective is called out in the following example:

[Objective 1: Provide context and meaning]

The 21st century environment of connected technologies offers us many exciting present and future opportunities. Unfortunately, there are those who seek to exploit these opportunities for personal, financial, or political gain. We, as an organization, are committed to protecting our clients, employees, stakeholders, business partners, and community from harm and to providing exceptional service.

The objective of our Information Security Policy is to protect and respect the confidentiality, integrity, and availability of client information, company proprietary data, and employee data, as well as the infrastructure that supports our services and business activities.

This policy has been designed to meet or exceed applicable federal and state information security–related regulations, including but not limited to sections 501 and 505(b) of the Gramm-Leach-Bliley Act (GLBA) and MA CMR 17 201 as well as our contractual obligations.

The scope of the Information Security Policy extends to all functional areas and all employees, directors, consultants, contractors, temporary staff, co-op students, interns, partners and third-party employees, and joint venture partners, unless explicitly excluded.

[Objective 2: Convey the importance of understanding and adhering to the policy]

Diligent information security practices are a civic responsibility and a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee and affiliate to know, understand, and adhere to these policies, and to conduct their activities accordingly. If you have any questions or would like more information, I encourage you to contact our Compliance Officer at x334.

[Objective 3: Acquaint the reader with the document and its contents]

At first glance, the policy [or policies, if you are using singular policy documents] may appear daunting. If you take a look at the table of contents [or list, if you are using singular policy documents] you will see that the Information Security Policy is organized by category. These categories form the framework of our Information Security Program. Supporting the policies are implementation standards, guidelines, and procedures. You can find these documents in the Governance section of our online company library.

[Objective 4: Explain the consequence of noncompliance as well as the exception process]

Where compliance is not technically feasible or justified by business needs, an exemption may be granted. Exemption requests must be submitted in writing to the Chief Operating Officer (COO), including justification and benefits attributed to the exemption. Unless otherwise stated, the COO and the President have the authority to grant waivers.

Willful violation of this policy [or policies, if you are using singular policy documents] may result in disciplinary action, which may include termination for employees and temporaries, a termination of employment relations in the case of contractors and consultants, and dismissal for interns and volunteers. Additionally, individuals may be subject to civil and criminal prosecution.

[Objective 5: Thank the reader and provide a seal of authority]

I thank you in advance for your support, as we all do our best to create a secure environment and to fulfill our mission.

—J. Johnson, Chief Executive Officer (CEO)

Policy Heading

A ***policy heading*** identifies the policy by name and provides the reader with an overview of the policy topic or category. The format and contents of the heading significantly depend on the format (singular or consolidated) you are using.

- Singular policies must be able to stand on their own, which means it is necessary to include significant logistical detail in each heading. The information contained in a singular policy heading may include the organization or division name, category (section), subsection, policy number, name of the author, version number, approval authority, effective date of the policy, regulatory cross-reference, and a list of supporting resources and source material. The topic is generally self-explanatory and does not require an overview or explanation.
- In a consolidated policy document, the heading serves as a section introduction and includes an overview. Because the version number, approval authority, and effective date of the policy have been documented in the version control table, it is unnecessary to include them in section headings. Regulatory cross-reference (if applicable), lead author, and supporting documentation are found in the Administrative Notation section of the policy.

In Practice

Policy Heading

A consolidated **policy heading** serves as the introduction to a section or category.

Section 1: Governance and Risk Management

Overview

Governance is the set of responsibilities and practices exercised by the Board of Directors and management team with the goal of providing strategic direction, ensuring that organizational objectives are achieved, risks are managed appropriately, and enterprise resources are used responsibly. The principal objective of an organization’s risk management process is to provide those in leadership and data steward roles with the information required to make well-informed decisions.

Policy Goals and Objectives

Policy goals and objectives act as a gateway to the content to come and the security principle they address. This component should concisely convey the intent of the policy. Note that even a singular policy can have multiple objectives. We live in a world where business matters are complex and interconnected, which means that a policy with a single objective might risk not covering all aspects of a particular situation. It is therefore important, during the planning phase, to pay appropriate attention to the different objectives the security policy should seek to achieve.

- Singular policies list the goals and objectives either in the policy heading or in the body of the document.
- In a consolidated policy document, the goals and objectives are grouped and follow the policy heading.

In Practice

Policy Goals and Objectives

Goals and objectives should convey the intent of the policy. Here's an example:

Goals and Objectives for Section 1: Governance and Risk Management

- To demonstrate our commitment to information security
- To define organizational roles and responsibilities
- To provide the framework for effective risk management and continuous assessment
- To meet regulatory requirements

Policy Statement

Up to this point in the document, we have discussed everything but the actual policy statement. The ***policy statement*** is best thought of as a high-level directive or strategic roadmap. This is the section where we lay out the rules that need to be followed and, in some cases, reference the implementation instructions (standards) or corresponding plans. Policy statements are intended to provide action items as well as the framework for situational responses. Policies are mandatory. Deviations or exceptions must be subject to a rigorous examination process.

In Practice

Policy Statement

The bulk of the final policy document is composed of policy statements. Here is an example of an excerpt from a governance and risk management policy:

1.1 Roles and Responsibilities

1.1.1 The Board of Directors will provide direction for and authorize the Information Security Policy and corresponding program.

1.1.2 The Chief Operating Officer (COO) is responsible for the oversight of, communication related to, and enforcement of the Information Security Policy and corresponding program.

1.1.3 The COO will provide an annual report to the Board of Directors that provides them with the information necessary to measure the organizations' adherence to the Information Security Policy objectives and to gauge the changing nature of risk inherent in lines of business and operations.

1.1.4 The Chief Information Security Officer (CISO) is charged with the implementation of the Information Security Policy and standards including but not limited to:

- Ensuring that administrative, physical, and technical controls are selected, implemented, and maintained to identify, measure, monitor, and control risks, in accordance with applicable regulatory guidelines and industry best practices
- Managing risk assessment–related remediation
- Authorizing access control permissions to client and proprietary information
- Reviewing access controls permissions in accordance with the audit standard
- Responding to security incidents

1.1.5 In-house legal counsel is responsible for communicating to all contracted entities the information security requirements that pertain to them as detailed within the Information Security Policy and the Vendor Management Program.

Policy Exceptions and the Exemption Process

Realistically, there will be situations where it is not possible or practical, or perhaps may even be harmful, to obey a policy directive. This does not invalidate the purpose or quality of the policy. It just means that some special situations will call for ***exceptions*** to the rule. ***Policy exceptions*** are agreed waivers that are documented within the policy. For example, in order to protect its intellectual property, Company A has a policy that bans digital cameras from all company premises. However, a case could be made that the HR department should be equipped with a digital camera to take pictures of new employees to paste them on their ID badges. Or maybe the Security Officer should have a digital camera to document the proceedings of evidence gathering after a security breach has been detected. Both examples are valid reasons why a digital camera might be needed. In these cases, an exception to the policy could be added to the document. If no exceptions are ever to be allowed, this should be clearly stated in the Policy Statement section as well.

An ***exemption*** or ***waiver process*** is required for exceptions identified after the policy has been authorized. The exemption process should be explained in the introduction. The criteria or conditions for exemptions should not be detailed in the policy, only the method or process for requesting an exemption. If we try to list all the conditions to which exemptions apply, we risk creating a loophole in the exemption itself. It is also important that the process follow specific criteria under which exemptions are granted or rejected. Whether an exemption is granted or rejected, the requesting party should be given a written report with clear reasons either way.

Finally, it is recommended to keep the number of approved exceptions and exemptions low, for several reasons:

- Too many built-in exceptions may lead employees to perceive the policy as unimportant.
- Granting too many exemptions may create the impression of favoritism.
- Exceptions and exemptions can become difficult to keep track of and successfully audit.

If there are too many built-in exceptions and/or exemption requests, it may mean that the policy is not appropriate in the first place. At that point, the policy should be subject to review.

In Practice

Policy Exception

Here's a policy exception that informs the reader who is not required to conform to a specific clause and under what circumstances and whose authorization:

"At the discretion of in-house legal counsel, contracted entities whose contracts include a confidentiality clause may be exempted from signing nondisclosure agreements."

The process for granting post-adoption exemptions should be included in the introduction. Here's an example:

"Where compliance is not technically feasible or as justified by business needs, an exemption may be granted. Exemption requests must be submitted in writing to the COO, including justification and benefits attributed to the exemption. Unless otherwise stated, the COO and the President have the authority to grant waivers."

Policy Enforcement Clause

The best way to deliver the message that policies are mandatory is to include the penalty for violating the rules. The ***policy enforcement clause*** is where the sanctions for non-adherence to the policy are unequivocally stated in order to reinforce the seriousness of compliance. Obviously, you must be careful with the nature of the penalty. It should be proportional to the rule that was broken, whether it was accidental or intentional and the level of risk the company incurred.

An effective method of motivating compliance is proactive training. All employees should be trained in the acceptable practices presented in the security policy. Without training, it is hard to fault employees for not knowing they were supposed to act in a certain fashion. Imposing disciplinary actions in such situations can adversely affect morale. We will take a look at various training, education, and awareness tools and techniques in later chapters.

In Practice

Policy Enforcement Clause

This example of a policy enforcement clause advises the reader, in no uncertain terms, what will happen if they do not obey the rules. It belongs in the introduction and, depending on the circumstances, may be repeated within the policy document.

"Violation of this policy may result in disciplinary action, which may include termination for employees and temporaries, a termination of employment relations in the case of contractors and consultants, and dismissal for interns and volunteers. Additionally, individuals are subject to civil and criminal prosecution."

Administrative Notations

The purpose of ***administrative notations*** is to refer the reader to additional information and/or provide a reference to an internal resource. Notations include regulatory cross-references, the name of corresponding documents such as standards, guidelines, and programs, supporting documentation such as annual reports or job descriptions, and the policy author's name and contact information. You should only include notations that are applicable to your organization. However, you should be consistent across all policies.

- Singular policies incorporate administrative notations either in the heading, at the end of the document, or split between the two locations. How this is handled depends on the policy template used by the company.
- In a consolidated policy document, the administrative notations are located at the end of each section.

In Practice

Administrative Notations

Administrative notations are a reference point for additional information. If the policy is distributed in electronic format, it is a great idea to hyperlink the notations directly to the source document.

Regulatory Cross Reference
Section 505(b) of the Gramm-Leach-Bliley Act
MA CMR 17 201

Lead Author
B. Lin, Chief Information Officer
b.lin@companya.com

Corresponding Documents
Risk Management Standards

Vendor Management Program
Supporting Documentation
Job descriptions as maintained by the Human Resources Department.

Policy Definitions

The Policy Definition section is a glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with. Adding definitions to the overall document will aid the target audience in understanding the policy, and will therefore make the policy a much more effective document.

The rule of thumb is to include definitions for any instance of industry-specific, technical, legal, or regulatory language. When deciding what terms to include, it makes sense to err on the side of caution. The purpose of the security policy as a document is communication and education. The target audience for this document usually encompasses all employees of the company, and sometimes outside personnel. Even if some technical topics are well known to all in-house employees, some of those outside individuals who come in contact with the company—and therefore are governed by the security policy—may not be as well versed in the policy's technical aspects.

Simply put, before you begin writing down definitions, it is recommended to first define the target audience for whom the document is crafted, and cater to the lowest common denominator to ensure optimum communication efficiency.

Another reason why definitions should not be ignored is for the legal ramification they represent. An employee cannot pretend to have thought that a certain term used in the policy meant one thing when it is clearly defined in the policy itself. When you're choosing which words will be defined, therefore, it is important not only to look at those that could clearly be unknown, but also those that should be defined to remove any and all ambiguity. A security policy could be an instrumental part of legal proceedings and should therefore be viewed as a legal document and crafted as such.

In Practice

Terms and Definitions

Any term that may not be familiar to the reader or is open to interpretation should be defined.

Here's an example of an abbreviation:

- MOU—Memorandum of Understanding

Here's an example of a regulatory reference:

- MA CMR 17 201—Standards for the Protection of Personal Information of Residents of the Commonwealth establishes minimum standards to be met in connection with the safeguarding of personal information of Massachusetts residents.

And, finally, here's an example of a security term:

- Distributed Denial of Service (DDoS)—A Distributed Denial of Service attack is designed to cripple a device by consuming all available resources.

Writing Style and Technique

Style is critical. The first impression of a document is based on its style and organization. If the reader is immediately intimated, the contents become irrelevant. Keep in mind that the role of policy is to guide behavior. That can only happen if the roadmap is clear and easy to use. How the document flows and the words you use will make all the difference as to how the policy is interpreted. Know your intended reader and write in a way that is understandable. Use terminology that is relevant. Most importantly, keep it simple. Polices that are overly complex tend to be misinterpreted. Policies should be written using plain language.

Using Plain Language

The term ***plain language*** means using the simplest, most straightforward way to express an idea.

No one technique defines plain language. Rather, plain language is defined by results—it is easy to read, understand, and use. Studies have proven that documents created using plain-language techniques are effective in a number of ways:[1]

- Readers understand documents better.
- Readers prefer plain language.
- Readers locate information faster.
- Documents are easier to update.
- It is easier to train people.
- Plain language saves time and money.

Even confident readers appreciate plain language. It enables them to read more quickly and with increased comprehension. The use of plain language is spreading in many areas of American culture, including governments at all levels, especially the federal government, healthcare, the sciences, and the legal system.

FYI: Warren Buffet on Using Plan Language

The following is excerpted from the preface to the Securities and Exchange Commission's *A Plain English Handbook*:

"For more than forty years, I've studied the documents that public companies file. Too often, I've been unable to decipher just what is being said or, worse yet, had to conclude that nothing was being said.

"Perhaps the most common problem, however, is that a well-intentioned and informed writer simply fails to get the message across to an intelligent, interested reader. In that case, stilted jargon and complex constructions are usually the villains.

"One unoriginal but useful tip: Write with a specific person in mind. When writing Berkshire Hathaway's annual report, I pretend that I'm talking to my sisters. I have no trouble picturing them: Though highly intelligent, they are not experts in accounting or finance. They will understand plain English, but jargon may puzzle them. My goal is simply to give them the information I would wish them to supply me if our positions were reversed. To succeed, I don't need to be Shakespeare; I must, though, have a sincere desire to inform.

"No siblings to write to? Borrow mine: Just begin with 'Dear Doris and Bertie.'"

Source: Securities and Exchange Commission, "A Plain English Handbook: How to create clear SEC disclosure documents," www.sec.gov/news/extra/handbook.htm.

The Plain Language Movement

It seems obvious that everyone would want to use plain language, but as it turns out, that is not the case. There is an enduring myth that in order to appear official or important, documents should be verbose. The result has been a plethora of complex and confusing regulations, contracts, and, yes, policies. In response to public frustration, the Plain Language Movement began in earnest in the early 1970s.

In 1971, the National Council of Teachers of English in the U.S. formed the Public Doublespeak Committee. In 1972, U.S. President Richard Nixon created plain language momentum when he decreed that the "Federal Register be written in 'layman's terms.'" The next major event in the U.S. history of plain language occurred in 1978, when U.S. President Jimmy Carter issued Executive Orders 12,044 and 12,174. The intent was to make government regulations cost-effective and easy to understand. In 1981, U.S. President Ronald Reagan rescinded Carter's executive orders. Nevertheless, many continued their efforts to simplify documents; by 1991, eight states had passed statutes related to plain language.

In 1998, then-President Clinton issued a Presidential Memorandum requiring government agencies to use plain language in communications with the public. All subsequent administrations have supported this memorandum. In 2010, plain language advocates achieved a major victory when the Plain Writing Act was passed. This law requires federal government agencies to write publications and forms in a "clear, concise, well-organized" manner using plain language guidelines.

We can take a cue from the government and apply these same techniques when writing policies, standards, guidelines, and plans. The easier a policy is to understand, the better the chance of compliance.

FYI: Plain Language Results

Here's an example of using plain language that involves the Pacific Offshore Cetacean Take Reduction Plan: Section 229.31. Not only did the National Marine Fisheries Service (NMFS) improve the language of this regulation, they turned the critical points into a user-friendly quick reference card, made it bright yellow so it's easy to find, and laminated it to stand up to wet conditions.

Before

After notification of NMFS, this final rule requires all CA/OR DGN vessel operators to have attended one Skipper Education Workshop after all workshops have been convened by NMFS in September 1997. CA/OR DGN vessel operators are required to attend Skipper Education Workshops at annual intervals thereafter, unless that requirement is waived by NMFS. NMFS will provide sufficient advance notice to vessel operators by mail prior to convening workshops.

After

After notification from NMFS, vessel operators must attend a skipper education workshop before commencing fishing each fishing season.

Source: www.plainlanguage.gov/examples/before_after/regfisheries.cfm

Plain Language Techniques for Policy Writing

The Plain Language Action and Information Network (PLAIN) describes itself on its website (http://plainlanguage.gov) as a group of federal employees from many different agencies and specialties, who support the use of clear communication in government writing. In March of 2011, PLAIN published the Federal Plain Language Guidelines. Some of the guidelines are specific to government publications. Many are applicable to both government and industry. The ten guidelines, listed here, are pertinent to writing policies and companion documents:

1. Write for your audience. Use language your audience knows and is familiar with.
2. Write short sentences. Express only one idea in each sentence.
3. Limit a paragraph to one subject. Aim for no more than seven lines.
4. Be concise. Leave out unnecessary words. Instead of, "for the purpose of," use "to." Instead of, "due to the fact," use "because."
5. Don't use jargon or technical terms when everyday words have the same meaning.
6. Use active voice. A sentence written in the active voice shows the subject acting in standard English sentence order: subject-verb-object. Active voice makes it clear who is supposed to do what. It eliminates ambiguity about responsibilities. Not "It must be done" but "You must do it."
7. Use "must" not "shall" to indicate requirements. "Shall" is imprecise. It can indicate either an obligation or a prediction. The word "must" is the clearest way to convey to your audience that they have to do something.
8. Use words and terms consistently throughout your documents. If you use the term "senior citizens" to refer to a group, continue to use this term throughout your document. Don't substitute another term, such as "the elderly" or "the aged." Using a different term may cause the reader to wonder if you are referring to the same group.

9. Omit redundant pairs or modifiers. For example, instead of “cease and desist,” use either “cease” or “desist.” Even better, use a simpler word such as “stop.” Instead of saying “the end result was the honest truth,” say “the result was the truth.”

10. Avoid double negatives and exceptions to exceptions. Many ordinary words have a negative meaning, such as unless, fail to, notwithstanding, except, other than, unlawful (“un-” words), disallowed (“dis-” words), terminate, void, insufficient, and so on. Watch out for them when they appear after “not.” Find a positive word to express your meaning.

Want to learn more about using plain language? The official website of PLAIN has a wealth of resources, including the Federal Plain Language Guidelines, training materials and presentations, videos, posters, and references.

In Practice

Understanding Active and Passive Voice

Here are some key points to keep in mind concerning active and passive voice:

- Voice refers to the relationship of a subject and its verb.
- Active voice refers to a verb that shows the subject acting.
- Passive voice refers to a verb that shows the subject being acted upon.

Active Voice

A sentence written in the active voice shows the subject acting in standard English sentence order: subject-verb-object. The subject names the agent responsible for the action, and the verb identifies the action the agent has set in motion. Example: “George threw the ball.”

Passive Voice

A sentence written in the passive voice reverses the standard sentence order. Example: “The ball was thrown by George.” George, the agent, is no longer the subject but now becomes the object of the preposition “by.” The ball is no longer the object but now becomes the subject of the sentence, where the agent preferably should be.

Conversion Steps

To convert a passive sentence into an active one, take these steps:

1. Identify the agent.
2. Move the agent to the subject position.
3. Remove the helping verb (to be).
4. Remove the past participle.
5. Replace the helping verb and participle with an action verb.

Examples of Conversion

Original: The report has been completed.

Revised: Jack completed the report.

Original: A decision will be made.

Revised: Jill will decide.

Source: United States Army Training and Doctrine Command, Action Officer Development Course, Staff Writing Module, made available to Plain Language Action Network and others interested in improving their power of expression.

In Practice

U.S. Army Clarity Index

The Clarity Index was developed to encourage plain writing. The index has two factors: average number of words per sentence and percentage of words longer than three syllables. The index adds together the two factors. The target is an average of 15 words per sentence and with 15% of the total text composed of three syllables or less. A resulting index between 20 and 40 is ideal and indicates the right balance of words and sentence length. In the following example (excerpted from Warren Buffet's SEC introduction), the index is composed of an average of 18.5 words per sentence, and 11.5% of the words are three syllables or more. An index of 30 falls squarely in the ideal range!

Sentence	Number of Words per Sentence	Number and Percentage of Words with Three or More Syllables
"For more than forty years, I've studied the documents that public companies file.	13	Two words: 2/13 = 15%
Too often, I've been unable to decipher just what is being said or, worse yet, had to conclude that nothing was being said.	23	One word: 1/23 = 4%
Perhaps the most common problem, however, is that a well-intentioned and informed writer simply fails to get the message across to an intelligent, interested reader.	26	Three words: 3/26= 11%
In that case, stilted jargon and complex constructions are usually the villains."	12	One word 2/12= 16%
Total	74	46%
Average	18.5	11.5%
Clarity Index	**18.5 + 11.5 = 30**	

Summary

You now know that policies need supporting documents to give them context and meaningful application. Standards, guidelines, and procedures provide a means to communicate specific ways to implement our policies. We create our organizational standards, which specify the requirements for each policy. We offer guidelines to help people comply with standards. We create sets of instructions known as procedures so tasks are consistently performed. The format of our procedure—Simple Step, Hierarchical, Graphic, or Flowchart—depends on the complexity of the task and the audience. In addition to our policies, we create plans or programs to provide strategic and tactical instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain timeframe, usually with defined stages and with designated resources.

Writing policy documents is a multistep process. First, we need to define the audience for which the document is intended. Then, we choose the format. Options are to write each policy as a discrete document (singular policy) or to group like policies together (consolidated policy). Lastly, we need to decide upon the structure, including the components to include and in what order.

The first and arguably most important section is the introduction. This is our opportunity to connect with the reader and to convey the meaning and important of our policies. The introduction should be written by the "person in charge," such as the CEO or President. This person should use the introduction to reinforce company-guiding principles and correlate them with the rules introduced in the security policy.

Specific to each policy are the heading, goals and objectives, the policy statement, and (if applicable) exceptions. The ***heading*** identifies the policy by name and provides the reader with an overview of the policy topic or category. The goals and objectives convey what the policy is intended to accomplish. The policy statement is where we lay out the rules that need to be followed and, in some cases, reference the implementation instructions (standards) or corresponding programs. Policy exceptions are agreed waivers that are documented within the policy.

An exemption or waiver process is required for exceptions identified after a policy has been authorized. The ***policy enforcement clause*** is where the sanctions for willful non-adherence to the policy are unequivocally stated in order to reinforce the seriousness of compliance. Administrative notations refer the reader to additional information and/or provide a reference to an internal resource. ***The policy definition section*** is a glossary of terms, abbreviations, and acronyms used in the document that the reader may be unfamiliar with.

Recognizing that the first impression of a document is based on its style and organization, we studied the work of the Plain Language Movement. Our objective for using plain language is to produce documents that are easy to read, understand, and use. We looked at ten techniques from the Federal Plain Language Guideline that we can (and should) use for writing effective policies. In the next section of the book, we put these newfound skills to use.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. The policy hierarchy is the relationships between which of the following?

   A. Guiding principles, regulations, laws, and procedures
   B. Guiding principles, standards, guidelines, and procedures
   C. Guiding principles, instructions, guidelines, and programs
   D. None of the above

2. Which of the following statements best describes the purpose of a standard?

   A. To state the beliefs of an organization
   B. To reflect the guiding principles
   C. To dictate mandatory requirements
   D. To make suggestions

3. Which of the following statements best describes the purpose of a guideline?

   A. To state the beliefs of an organization
   B. To reflect the guiding principles
   C. To dictate mandatory requirements
   D. To make suggestions

4. Which of the following statements best describes the purpose of a baseline?

   A. To measure compliance
   B. To ensure uniformity across a similar set of devices
   C. To ensure uniformity across different devices
   D. To make suggestions

5. Simple Step, Hierarchical, Graphic, and Flowchart are examples of which of the following formats?

   A. Policy
   B. Program
   C. Procedure
   D. Standard

6. Which of the following terms best describes instructions and guidance on how to execute an initiative or how to respond to a situation, within a certain timeframe, usually with defined stages and with designated resources?

   A. Plan

   B. Policy

   C. Procedure

   D. Package

7. Which of the following statements best describes a disadvantage to using the singular policy format?

   A. The policy can be short.

   B. The policy can be targeted.

   C. You may end up with too many policies to maintain.

   D. The policy can easily be updated.

8. Which of the following statements best describes a disadvantage to using the consolidated policy format?

   A. Consistent language is used throughout the document.

   B. Only one policy document must be maintained.

   C. The format must include a composite management statement.

   D. The potential size of the document.

9. Policies, standards, guidelines, and procedures should all be in the same document.

   A. True

   B. False

   C. Only if the company is multinational

   D. Only if the documents have the same author

10. Version control is the management of changes to a document and should include which of the following elements?

   A. Version or revision number

   B. Date of authorization

   C. Change description

   D. All of the above

11. Which of the following is not a policy introduction objective?

- **A.** To convey the importance of understanding and adhering to the policy
- **B.** To provide explicit instructions on how to comply with the policy
- **C.** To explain the exemption process as well as the consequence of non-compliance
- **D.** To thank the reader and to reinforce the authority of the policy

12. The name of the policy, policy number, and overview belong in which of the following sections?

- **A.** Introduction
- **B.** Policy Heading
- **C.** Policy Goals and Objectives
- **D.** Policy Statement

13. The aim or intent of a policy is stated in the ________.

- **A.** introduction
- **B.** policy heading
- **C.** policy goals and objectives
- **D.** policy statement

14. Which of the following statements is true?

- **A.** A security policy should only include one objective.
- **B.** A security policy should not include any exceptions.
- **C.** A security policy should not include a glossary.
- **D.** A security policy should not list all step-by-step measures that need to be taken.

15. The _________ contains the rules that must be followed.

- **A.** policy heading
- **B.** policy statement
- **C.** policy enforcement clause
- **D.** policy goals and objectives

16. A policy should be considered _____.

- **A.** mandatory
- **B.** discretionary
- **C.** situational
- **D.** optional

17. Which of the following best describes policy definitions?

    A. A glossary of terms used

    B. A detailed list of the possible penalties associated with breaking rules set forth in the policy

    C. A list of all the members of the security policy creation team

    D. None of the above

18. The _________ contains the penalties that would apply if a portion of the security policy were to be ignored by an employee.

    A. policy heading

    B. policy statement

    C. policy enforcement clause

    D. policy statement of authority

19. What component of a security policy does the following phrase belong to? “Wireless networks are allowed only if they are separate and distinct from the corporate network.”

    A. Introduction

    B. Administrative notation

    C. The policy heading

    D. The policy statement

20. There may be situations where it is not possible to comply with a policy directive. Where should the exemption or waiver process be explained?

    A. Introduction

    B. The policy statement

    C. The policy enforcement clause

    D. The policy exceptions

21. The name of the person/group (for example, executive committee) that authorized the policy should be included in ____________________.

    A. the version control table or the policy statement

    B. the heading or the policy statement

    C. the policy statement or the policy exceptions

    D. the version control table or the policy heading

22. When you're drafting a list of exceptions for a security policy, the language should ________________.

A. be as specific as possible

B. be as vague as possible

C. reference another, dedicated document

D. None of the above

23. If supporting documentation would be of use to the reader, it should be ________________.

A. included in full in the policy document

B. ignored because supporting documentation does not belong in a policy document

C. listed in either the Policy Heading or Administrative Notation section

D. included in a policy appendix

24. When writing a policy, standard, guideline, or procedure, you should use language that is __________.

A. technical

B. clear and concise

C. legalese

D. complex

25. Readers prefer "plain language" because it ________________.

A. helps them locate pertinent information

B. helps them understand the information

C. saves time

D. All of the above

26. Which of the following is not a characteristic of plain language?

A. Short sentences

B. Using active voice

C. Technical jargon

D. Seven or fewer lines per paragraph

27. Which of the following terms is best to use when indicating a mandatory requirement?

A. must

B. shall

C. should not

D. may not

28. A company that uses the term "employees" to refer to workers who are on the company payroll should refer to them throughout their policies as _________.

    A. workforce members
    B. employees
    C. hired hands
    D. workers

29. "The ball was thrown by Sam to Sally" is a passive sentence. Which of the following sentences represents an active version of this sentence?

    A. The ball was thrown to Sally by Sam.
    B. Sally caught the ball.
    C. Sam threw the ball to Sally.
    D. The ball was thrown by Sam to Sally, who caught it.

30. Even the best-written policy will fail if which of the following is true?

    A. The policy is too long.
    B. The policy is mandated by the government.
    C. The policy doesn't have the support of management.
    D. All of the above.

EXERCISES

EXERCISE 2.1: Creating Standards, Guidelines, and Procedures

The University System has a policy that states "All students must comply with their campus attendance standard."

1. You are tasked with developing a standard that documents the mandatory requirements (for example, how many classes can be missed without penalty). Include at least four requirements.
2. Create a guideline to help students adhere to the standard you created.
3. Create a procedure for requesting exemptions to the policy.

EXERCISE 2.2: Writing Policy Statements

1. Who would be the target audience for a policy related to campus elections?
2. Keeping in mind the target audience, compose a policy statement related to campus elections.
3. Compose an enforcement clause.

EXERCISE 2.3: Writing a Policy Introduction

1. Write an introduction to the policy you created in Exercise 2.2.
2. Generally an introduction is signed by an authority. Who would be the appropriate party to sign the introduction?
3. Write an exception clause.

EXERCISE 2.4: Writing Policy Definitions

1. The purpose of policy definitions is to clarify ambiguous terms. If you were writing a policy for an on-campus student audience, what criteria would you use to determine which terms should have definitions?
2. What are some examples of terms you would define?

EXERCISE 2.5: Using Clear Language

1. Identify the passive verb in each of the following lines. Hint: Test by inserting a subject (for example, he or we) before the verb.

a)	was written	will write	has written	is writing
b)	shall deliver	may deliver	is delivering	is delivered
c)	has sent	were sent	will send	is sending
d)	should revoke	will be revoking	has revoked	to be revoked
e)	is mailing	have been mailed	having mailed	will mail
f)	may be requesting	are requested	have requested	will request

2. Shorten the following phrases (for example, “Consideration should be given to” can be shortened to “consider”).

	Original	**Modified**
a)	For the purpose of	To
b)	Due to the fact that	Because
c)	Forwarded under separate cover	Sent separately

3. Delete the redundant modifiers (for example, for “actual facts,” you would delete the word “actual”):

a) Honest truth

b) End result

c) Separate out

d) Start over again

e) Symmetrical in form

f) Narrow down

PROJECTS

PROJECT 2.1: Categorizing a Real Security Policy

1. Search online for "Tufts University Information Technology Resources Security Policy."
2. Read the document. Identify the policy components that were covered in this chapter.
3. What is the last modified date of the policy? Does the date influence your opinion of the policy?
4. Choose a couple terms in the policy that are not defined in the Policy Definitions section and write a definition for each.

PROJECT 2.2: Analyzing the Enterprise Security Policy for the State of New York

1. Search online for the "State of New York Cyber Security Policy P03-002" document.
2. Read the policy. What is your overall opinion of the policy?
3. What is the purpose of the italic format? In your opinion, is it useful or distracting?
4. The reference to the "Definitions and Acronyms" document in the policy is incorrect. The correct reference is www.dhses.ny.gov/ocs/resources/documents/Definitions-Acronyms.pdf. What are the pros and cons of having a single glossary?
5. The policy references standards and procedures. Identify at least one instance of each. Can you find any examples of where a standard, guideline, or procedure is embedded in the policy document?

PROJECT 2.3: Testing the Clarity of a Policy Document

1. Locate your school's information security policy. (It may have a different name.)
2. Select a section of the policy and use the U.S. Army's Clarity Index to evaluate the ease of reading (reference the "In Practice: U.S. Army Clarity Index" sidebar for instructions).
3. Explain how you would make the policy more readable.

Case Study

Clean Up the Library Lobby

The library includes the following exhibition policy:

"Requests to utilize the entrance area at the library for the purpose of displaying posters and leaflets gives rise to the question of the origin, source, and validity of the material to be displayed. Posters, leaflets, and other display materials issued by the Office of Campus Security, Office of Student Life, the Health Center, and other authoritative bodies are usually displayed in libraries, but items of a fractious or controversial kind, while not necessarily excluded, are considered individually."

The lobby of the school library is a mess. Plastered on the walls are notes, posters, and cards of all sizes and shapes. It is impossible to tell current from outdated messages. It is obvious that no one is paying any attention to the library exhibition policy. You have been asked to evaluate the policy and make the necessary changes needed to achieve compliance.

1. Consider your audience. Rewrite the policy using plain language guidelines. You may encounter resistance to modifying the policy, so document the reason for each change, such as changing passive voice to active voice, eliminating redundant modifiers, and shortening sentences.
2. Expand the policy document to include goals and objectives, exceptions, and a policy enforcement clause.
3. Propose standards and guidelines to support the policy.
4. Propose how you would suggest introducing the policy, standards, and guidelines to the campus community.

References

[1] Baldwin, C. *Plain language and the document revolution*. Washington, D.C.: Lamplighter, 1999.

Regulations and Directives Cited

Carter, J. “Executive Order—Improving Government Regulations,” accessed 05/2013, www.presidency.ucsb.edu/ws/?pid=30539.

Clinton, W. “President Clinton’s Memorandum on Plain Language in Government Writing,” accessed 05/2013, www.plainlanguage.gov/whatisPL/govmandates/memo.cfm.

Obama, B. “Executive Order 13563—Improving Regulation and Regulatory Review,” accessed 05/2013, www.whitehouse.gov/the-press-office/2011/01/18/improving-regulation-and-regulatory-review-executive-order.

“Plain Writing Act of 2010” PUBLIC LAW 111–274, Oct. 13, 2010, accessed 05/2013, www.gpo.gov/fdsys/pkg/PLAW-111publ274/.../PLAW-111publ274.pdf.

Other References

Krause, Micki, CISSP, and Harold F. Tipton, CISSP. Information Security Management Handbook, Fifth Edition. Boca Raton, FL: CRC Press, Auerbach Publications, 2004.

“Tufts University Information Technology Resource Security Policy.” Tufts University, accessed 05/2013, www.tufts.edu/tccs/p-resourcesec1.shtml.

Smith, T. “State of New York, Cyber-Security Policy P03-002,” Office of CyberSecurity, accessed 05/2013, www.dhses.ny.gov/.../documents/Cyber-Security-Policy-P03-002-V3.4.pdf.

Smith, T. “State of New York, Cyber Security Policies, Standards and Guidelines Definitions & Acronyms,” accessed 05/20/2013, www.dhses.ny.gov/ocs/resources/documents/Definitions-Acronyms.pdf.

Official website of PLAIN, accessed 05/2013, www.plainlanguage.gov.

“Pacific Offshore Cetacean Take Reduction Plan: Section 229.31,” PLAIN, accessed 05/20/2013, www.plainlanguage.gov/examples/before_after/regfisheries.cfm.

“Federal Plan Language Guidelines,” PLAIN, accessed 05/2013, www.plainlanguage.gov/howto/guidelines/FederalPLGuidelines/index.cfm.

“Action Officer Development Course, Staff Writing Module,” United States Army Training and Doctrine Command, accessed 05/2013, www.plainlanguage.gov/resources/take_training/index.cfm.

Mazur, B. “Revisiting Plan Language,” accessed 05/2013, www.plainlanguage.gov/whatisPL/history/mazur.cfm. Originally published in the May 2000 (Vol. 47, No. 2) issue of *Technical Communication, The Journal of the Society for Technical Communication*.

Kimble, J. “The Elements of Plain Language,” accessed 05/2013, www.plainlanguage.gov/whatisPL/definitions/Kimble.cfm.

“Various Plain English Statutes,” accessed 05/2013, www.languageandlaw.org/TEXTS/STATS/PLAINENG.HTM.

“Before and After,” Plain English Campaign, accessed 05/2013, www.plainenglish.co.uk.

“The Writing Clarity Rating,” accessed 05/2013, www.infogineering.net/writing-clarity-rating.htm.

“A Plain English Handbook: How to Create Clear SEC Disclosure Documents,” Securities and Exchange Commission, accessed 05/2013, www.sec.gov/news/extra/handbook.htm.

“Resources for Trainers—Class Exercises and Answers,” accessed 05/2013, www.plainlanguage.gov/resources/for_trainers/PLAIN.cfm.

Buffet, W. Preface to the Securities and Exchange Commission’s “A Plain English Handbook: How to Create Clear SEC Disclosure Documents,” accessed 05/2013, www.sec.gov/news/extra/handbook.htm.

Chapter 3

Information Security Framework

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Recognize the importance of the CIA security model.
- Describe the security objectives of confidentiality, integrity, and availability.
- Discuss why organizations choose to adopt a security framework.
- Recognize the value of NIST resources.
- Understand the intent of the ISO/IEC 27000-series of information security standards.
- Outline the domains of an information security program.

Our focus in this chapter on information security objectives and framework will answer the following (and many other) questions associated with the need to maintain secure communications among and between government, public, and private sectors. In context, our efforts to sustain reliable and secure communications has become a worldwide global effort with cybersecurity.

- What are we trying to achieve in pursuit of information security?
- What is the ultimate goal of writing information security policies?
- What tangible benefit will come to our customers, our employees, our partners, and our organizations from our Herculean effort?

A framework lends itself to many easily related metaphors. The most obvious is that of any building: no foundation, no building. More specifically, the better the framing of any building, the longer it will last, the more it can hold, and the more functional it becomes. Of course, with any building there must first be a plan. We hire architects and engineers to design our buildings, to think about what is possible, and relay the best way to achieve those possibilities.

In the same way, we need a framework for our information security program. Much like the many rooms in a building, each with its own functions, we segment our information security program into logical and tangible units called domains. ***Security domains*** are associated with designated groupings of related activities, systems, or resources. For example, the Human Resources Security Management domain includes topics related to personnel, such as background checks, confidentiality agreements, and employee training. Without the framework, every new situation will see us repeating, redesigning, and reacting, which all together can be referred to as "unplanned," or spending time in crisis. Fortunately, in the information security arena there is absolutely no reason to choose crisis over preparedness. Strategies involving proactive, rather than reactive, procedures have become the ad hoc standard for systems of cybersecurity governance. A number of public and private organizations, including the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST), have all invested considerable time and energy to develop structures that we can draw upon.

In this chapter, you are going to be introduced to both. Before we begin building our information security program and policies, we need to first identify what we are trying to achieve and why. We will begin this chapter by discussing the three basic tenants of information security. We will then look at the escalating global threat, including who is behind the attacks, their motivation, and how they attack. We will apply this knowledge to building the framework of our information security program and how we write our policies.

CIA

CIA. It is easy to guess that the first thing that popped into your mind when you read those three letters was the Central Intelligence Agency. In the information security world, these three letters represent something we strive to attain rather than an agency of the United States government. Confidentiality, integrity, and availability (CIA) are the unifying attributes of an information security program. Collectively referred to as the ***CIA triad*** or ***CIA security model***, each attribute represents a fundamental objective of information security. The Federal Information Security Management Act (FISMA) defines the relationship between information security and the CIA triad as follows:

> (1) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
>
> > (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation, accuracy, and authenticity;
> >
> > (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
> >
> > (C) availability, which means ensuring timely and reliable access to and use of information.

You may be wondering which is most important: confidentiality, integrity, or availability? The answer requires an organization to assess its mission, evaluate its services, and consider regulations and contractual agreements. As Figure 3.1 illustrates, organizations may consider all three components of the CIA triad equally important, in which case resources must be allocated proportionately.

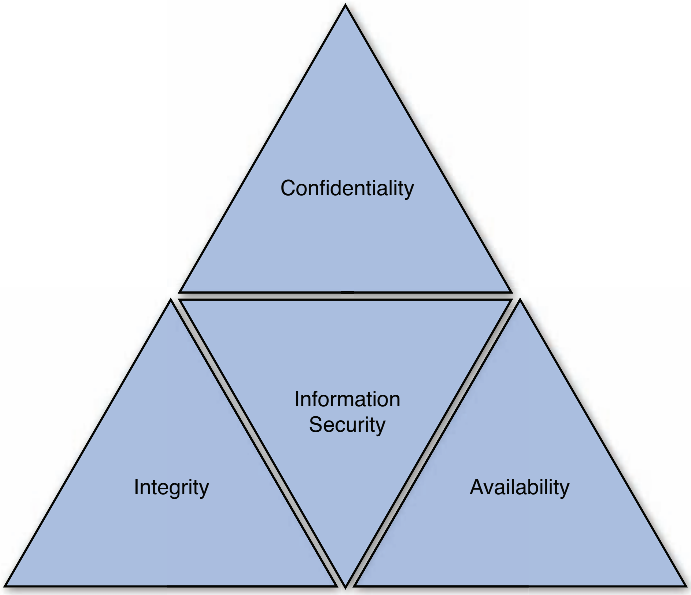


FIGURE 3.1 CIA triad.

What Is Confidentiality?

When you tell a friend something "in confidence," you expect them to keep the information private and to not share what you told them with anyone else without your permission. You also hope that they will never use this against you. Likewise, ***confidentiality*** is the requirement that private or confidential information not be disclosed to unauthorized individuals.

The information exchanged between doctors and patients or lawyers and clients is protected by confidentiality laws called the "doctor-patient privilege" and the "attorney-client privilege," respectively. We place a very high value on this quality in people and express it in many ways, referring to those who keep our confidences as trustworthy, dependable, or loyal. The confidentiality of information is certainly not a new idea, so what is all the fuss about?

Not only has the amount of information stored, processed, and transmitted on privately owned networks and the public Internet increased dramatically, so has the number of ways to potentially access the data. The Internet, its inherent weaknesses, and those willing (and able) to exploit vulnerabilities are the main reasons why protecting confidentiality has taken on a new urgency. The technology and accessibility we take for granted would have been considered magic just ten years ago. The amazing speed at which we arrived here is also the reason we have such a gap in security. The race to market often means that security is sacrificed. So although it may seem to some that information security requirements are a bit extreme at times, it is really a reaction to the threat environment.

As it pertains to information security, confidentiality is the protection of information from unauthorized people and processes. Federal Code 44 U.S.C., Sec. 3542 defines confidentiality as "preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information."

None of us likes the thought of our private health information or financial information falling into some stranger's hands. No business owner likes the thought of her proprietary business information being disclosed to competitors. Information is valuable. Social security numbers are used for identity theft. Bank account credentials are used to steal money. Medical insurance information can be used to fraudulently obtain services or to make counterfeit claims. Military secrets can be used to build weaponry, track troop movements, or expose counterintelligence agents. The list goes on and on.

FYI: The Enemy Within

Authorized access can be misused with dangerous, even deadly, consequences. Consider the case of U.S. Army Private Bradley Manning. Assigned to an army unit based near Baghdad, U.S. Army Private Bradley Manning held a Top Secret/SCI clearance and had access to documents on two classified networks: SIPRNET, the Top Secret–level network used by the Department of Defense and the State Department, and the Joint Worldwide Intelligence Communications System, which serves both agencies at the Top Secret/SCI level.

Manning downloaded classified material onto a CD. According to Manning, "I would come in with music on a CD-RW labeled with something like 'Lady Gaga,' erase the music, then write a compressed split file. No one suspected a thing and, odds are, they never will. I listened and lip-synced to Lady Gaga's 'Telephone' while exfiltrating possibly the largest data spillage in American history." The material included videos of the July 12, 2007 Baghdad airstrike and the 2009 Granai airstrike in Afghanistan; 250,000 United States diplomatic cables; and 500,000 army reports that came to be known as the Iraq War logs and Afghan War logs.

Manning provided the documents and videos to WikiLeaks, an organization that facilitates the anonymous leaking of secret information through its website. They describe themselves as follows: "WikiLeaks is a not-for-profit media organisation. Our goal is to bring important news and information to the public. We provide an innovative, secure and anonymous way for sources to leak information to our journalists (our electronic drop box)." The material provided by Manning was the largest set of restricted documents ever leaked to the public. WikiLeaks or its media partners published much of it between April and November 2010.

Manning was arrested on July 6, 2010. The U.S. military charged Manning with violating army regulations by transferring classified information to a personal computer and adding unauthorized software to a classified computer system as well as with violating federal laws of governing the handling of classified information. Asked how he got away with it, he said, "Weak servers, weak logging, weak physical security, weak counterintelligence, and inattentive signal analysis… a perfect storm."

Cybercrime is a relatively easy, low-risk, high-reward venture. There is plenty of money to be made. The chances of being caught are slim. The tools are readily available. Criminals look for and are prepared to exploit weaknesses in network designs, software, communication channels, and people. The opportunities are plentiful. Criminals are not always outsiders. Insiders can be tempted to "make copies" of information they have access to for financial gain, notoriety, or to "make a statement." The most recent threat to confidentiality is hacktivism, which is a combination of the terms "hack" and "activism." Hacktivism has been described as the fusion of hacking and activism, politics and technology. Hackitivist groups or collectives expose or hold hostage illegally obtained information to make a political statement or for revenge.

FYI: Hacktivism

A member of the Cult of the Dead Cow hacker collective named Omega first coined the term in 1996. If hacking as "illegally breaking into computers" is assumed, then hacktivism could be defined as "the use of legal and/or illegal digital tools in pursuit of political ends." These tools include website defacements, redirects, denial of service (DoS) attacks, information theft, website parodies, virtual sit-ins, typosquatting, and virtual sabotage.

The ability to obtain unauthorized access is often opportunistic. In this context, opportunistic means taking advantage of identified weaknesses. Criminals (and nosy employees) care about the work factor, which is defined as how much effort is needed to complete a task. The longer it takes to obtain unauthorized access, the greater the chance of being caught. The more a "job" costs to successfully complete, the less profit earned. The information security goal of confidentiality is to protect information from unauthorized access and misuse. The best way to do this is to implement safeguards and processes that increase the work factor and the chance of being caught. This calls for a spectrum of access controls and protections as well as ongoing monitoring, testing, and training.

What Is Integrity?

Whenever the word integrity comes to mind, so does Brian De Palma's classic 1987 film *The Untouchables*, starring Kevin Costner and Sean Connery. The film is about a group of police officers who could not be "bought off" by organized crime. They were incorruptible. Integrity is certainly one of the highest ideals of personal character. When we say someone has integrity, we mean she lives her life according to a code of ethics; she can be trusted to behave in certain ways in certain situations. It is interesting to note that those to whom we ascribe the quality of integrity can be trusted with our confidential information. As for information security, integrity has a very similar meaning. ***Integrity*** is the protection of information, processes, or systems from intentional or accidental unauthorized modification. In the same way we count on people of integrity to behave a certain way, we rely on our information to be a certain way.

Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. In other words, is the information the same as it was intended to be? For example, if you save a file with important information that must be relayed to members of your organization, but someone opens the file and changes some or all of the information, the file has lost its integrity. The consequences could be anything from coworkers missing a meeting you planned for a specific date and time, to 50,000 machine parts being produced with the wrong dimensions.

System integrity is a requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system." A computer virus that corrupts some of the system files required to "boot" the computer is an example of deliberate unauthorized manipulation.

Errors and omissions are an important threat to data and system integrity. These errors are caused not only by data entry clerks processing hundreds of transactions per day, but also by all types of users who create and edit data and code. Even the most sophisticated programs cannot detect all types of input errors or omissions. In some cases, the error is the threat, such as a data entry error or a programming error that crashes a system. In other cases, the errors create vulnerabilities. Programming and development errors, often called "bugs," can range in severity from benign to catastrophic.

To make this a bit more personal, let's talk about medical and financial information. What if you are injured, unconscious, and taken to the emergency room of a hospital, and the doctors need to look up your health information. You would want it to be correct, wouldn't you? Consider what might happen if you had an allergy to some very common treatment and this critical information had been deleted from your medical records. Or think of your dismay if you check your bank balance after making a deposit and find that the funds have not been credited to your account!

Integrity and confidentiality are interrelated. If a user password is disclosed to the wrong person, that person could in turn manipulate, delete, or destroy data after gaining access to the system with the password he obtained. Many of the same vulnerabilities that threaten integrity also threaten confidentiality. Most notable, though, is human error. Safeguards that protect against the loss of integrity include access controls such as encryption and digital signatures, process controls such as code testing, monitoring controls such as file integrity monitoring and log analysis, and behavioral controls such as separation of duties, rotation of duties, and training.

What Is Availability?

The final component of the CIA triad is also most often left out of consideration when one thinks about security. But, what does it mean to be secure? Would you feel secure if your car failed to start? Would you feel secure if you were very sick and your doctor could not be found? Whether or not systems and data are available for use is just as crucial as the confidentiality and integrity of the data itself. ***Availability*** is the assurance that systems and data are accessible by authorized users when needed. If we can't access the data we need, when we need it, we are not secure.

We must broaden our understanding of what information security means in several ways. For one (which was demonstrated earlier), information security is not just about computers—it is about information. For another, security does not pertain only to crime, malicious acts, or those who perpetrate them. It also pertains to feeling secure that the information can be used when needed, in the way needed.

In fact, availability is generally one of the first security issues addressed by Internet service providers (ISPs). You may have heard the expressions "uptime" and "5-9s" (99.999% uptime). This means the systems that serve Internet connections, web pages, and other such services will be available to users who need them when they need them. The ***service level agreement (SLA)*** is a type of agreement between a service provider and a customer that specifically addresses availability of services.

Just like confidentiality and integrity, we prize availability. We want our friends and family to "be there when we need them," we want food and drink available, we want our money available, and so forth. In some cases, our lives depend on the availability of these things, including information. Ask yourself how you would feel if you needed immediate medical care and your physician could not access your medical records.

Threats to availability include loss of processing ability due to natural disasters; hardware failures; programming errors; human error; injury, sickness, or death of key personnel; distributed denial of service (DDoS) attacks; and malicious code. We are more vulnerable to availability threats than to the other components of the CIA triad. We are certain to face some of them. Safeguards that address availability include access controls, monitoring, data redundancy, resilient systems, virtualization, server clustering, environmental controls, continuity of operations planning, and incident response preparedness.

FYI: Distributed Denial of Service Attacks

A DoS attack is an attempt to make a machine or network resource unavailable for its intended use. In general terms, DoS attacks consume computing resources or obstruct the communication channel.

As illustrated in Figure 3.2, a DDoS attack is one in which a multitude of compromised systems attack a single target. The flood of incoming requests to the target system essentially forces it to shut down, thereby denying service to legitimate users. There are multiple victims in a DDoS attack: the owners of the targeted systems, the users of the targeted system, and the owners of the compromised computers. A computer used in the attack is known as a bot. A group of co-opted computers is known as a botnet. Although the owners of co-opted computers are typically unaware that their computers have been compromised, they are nevertheless likely to suffer degradation of service and malfunction.

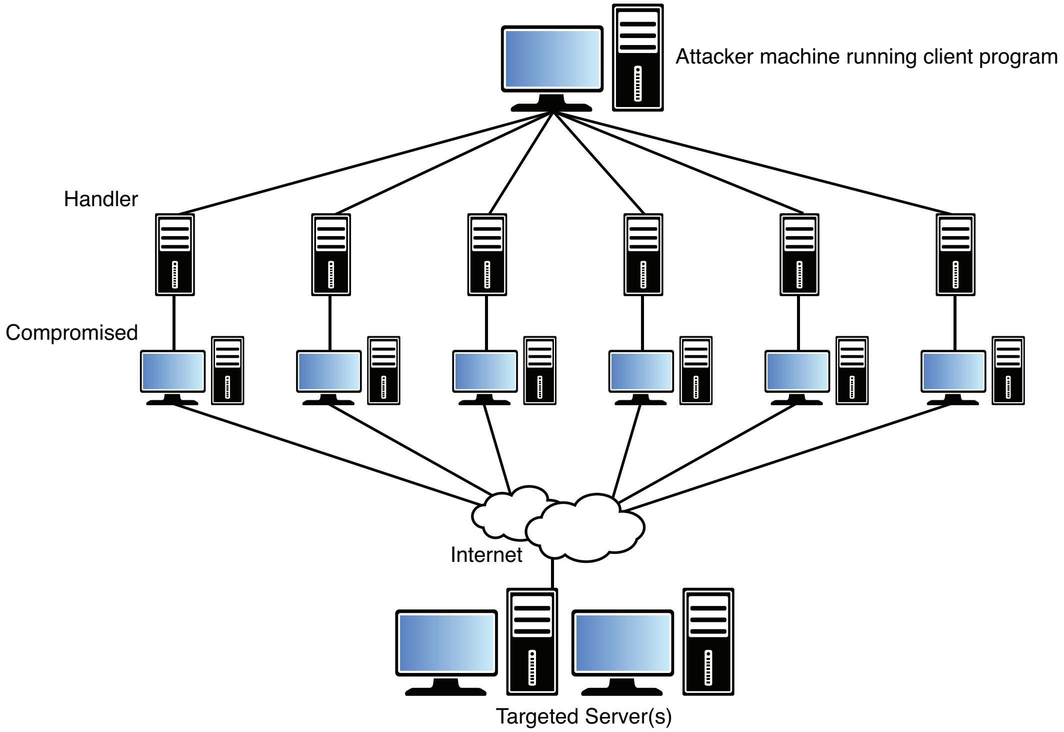


FIGURE 3.2 A conceptual diagram of a DDoS attack.

In Practice

The “Five A’s” of Information Security

Supporting the CIA triad of information security are five key information security principles, commonly known as the ***Five A’s***. Here is a quick explanation of each:

Accountability—The process of tracing actions to their source. Nonrepudiation techniques, intrusion detection systems (IDS), and forensics all support accountability.

Assurance—The processes, policies, and controls used to develop confidence that security measures are working as intended. Auditing, monitoring, testing, and reporting are the foundations of assurance.

Authentication—The positive identification of the person or system seeking access to secured information or systems. Password, Kerberos, token, and biometric are forms of authentication.

Authorization—Granting users and systems a predetermined level of access to information resources.

Accounting—The logging of access and usage of information resources.

CIA plus the Five A’s are fundamental objectives and attributes of an information security program.

Who Is Responsible for CIA?

It is the information owners' responsibility to ensure confidentiality, integrity, and availability. What does it mean to be an information owner? Under the FISMA Act of 2002, an information owner is an official with statutory or operational authority for specified information and responsibility for establishing the criteria for its creation, collection, processing, dissemination, or disposal, which may extend to interconnected systems or groups of interconnected systems. More simply, an ***information owner*** has the authority and responsibility for ensuring that information is protected, from creation through destruction. For example, a bank's senior loan officer might be the owner of information pertaining to customer loans. The senior loan officer has the responsibility to decide who has access to customer loan information, the policies for using this information, and the controls to be established to protect this information.

Information technology (IT) or information systems (IS) departments are widely perceived as owning the information and information systems. Perhaps this is due to the word "information" being part of the department title. For the record, with the exception of information specific to their department, IT and IS departments should not be considered information owners. Rather, they are the people charged with maintaining the systems that store, process, and transmit the information. They are known as ***information custodians***—those responsible for implementing, maintaining, and monitoring safeguards and systems. They are better known as system administrators, webmasters, and network engineers. We will be taking a closer look at each of these roles in the next chapter.

Information Security Framework

The best security minds in the world have contributed to researching, evaluating, and publishing security frameworks. ***Security framework*** is a collective term given to guidance on topics related to information systems security, predominantly regarding the planning, implementing, managing, and auditing of overall information security practices. Two of the most widely used frameworks are the Information Technology and Security Framework created by the United States ***NIST*** and the Information Security Management System offered by the ***ISO***. NIST offers well-documented procedures and programs to support secure information systems, whereas the ISO offers a certifiable method for integrating information security into the management process. When these frameworks are used in concert, an organization can create a comprehensive information security program.

What Is NIST's Function?

Founded in 1901, the NIST is a nonregulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve quality of life. The Computer Security Division (CSD) is one of eight divisions within NIST's Information Technology Laboratory. The mission of NIST's CSD is to improve information systems security as follows:

- By raising awareness of IT risks, vulnerabilities, and protection requirements, particularly for new and emerging technologies.
- By researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive federal systems.
- By developing standards, metrics, tests, and validation programs
  - to promote, measure, and validate security in systems and services, and
  - to educate consumers and to establish minimum security requirements for federal systems.
- By developing guidance to increase secure IT planning, implementation, management, and operation.

The 2002 E-Government Act [Public Law 107-347] assigned the NIST the mission of developing an Information Assurance Framework (standards and guidelines) designed for federal information systems that are not designated as national security systems. The NIST Information Assurance Framework includes the Federal Information Processing Standards (FIPS) and Special Publications (SP). Although developed for government use, the framework is applicable to the private sector and addresses the management, operational, and technical aspects of protecting the CIA of information and information systems.

NIST defines information security as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide CIA. Currently, there are more than 300 NIST information security–related documents. This number includes FIPS, the SP 800 series, information, Information Technology Laboratory (ITL) bulletins, and NIST interagency reports (NIST IR):

- **Federal Information Processing Standards (FIPS)**—This is the official publication series for standards and guidelines adopted and promulgated under the provisions of the FISMA Act of 2002.
- **Special Publication (SP) 800 series**—This series reports on ITL research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.
- **ITL bulletins**—Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis.

From access controls to wireless security, the NIST publications are truly a treasure trove of valuable and practical guidance.

What Does the ISO Do?

The ISO is a network of the national standards institutes of 146 countries. Each member country is allowed one delegate, and a Central Secretariat in Geneva, Switzerland coordinates the system. In 1946, delegates from 25 countries met in London and decided to create a new international organization, of which the objective would be "to facilitate the international coordination and unification of industrial standards." The new organization, ISO, officially began operations on February 23, 1947.

ISO is a nongovernmental organization: Unlike the United Nations, its members are not delegations of national governments. Nevertheless, ISO occupies a special position between the public and private sectors. This is because, on the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. ISO has developed more than 13,000 International Standards on a variety of subjects, ranging from country codes to passenger safety.

The ISO/IEC 27000 series (also known as the ISMS Family of Standards, or ISO27k for short) comprises information security standards published jointly by the ISO and the International Electrotechnical Commission (IEC).

The first six documents in the ISO/IEC 27000 series provide recommendations for "establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System." In all, there are 22 documents in the series, and several more are still under development.

- ISO 27001 is the specification for an Information Security Management System (ISMS).
- ISO 27002 describes the Code of Practice for information security management.
- ISO 27003 provides details implementation guidance.
- ISO 27004 outlines how an organization can monitor and measure security using metrics.
- ISO 27005 defines the high-level risk management approach recommended by ISO.
- ISO 27006 outlines the requirements for organizations that will measure ISO 27000 compliance for certification.

The framework is applicable to public and private organizations of all sizes. According to the ISO website, "the ISO standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings."

We are going to focus on the ISO 27002 Code of Practice. ISO 27002 has its origins in Great Britain. In 1989, the UK Department of Trade and Industry's (DTI's) Commercial Computer Security Centre (CCSC) developed the "Users Code of Practice," designed to help computer users employ sound security practices and ensure the CIA of information systems. Further development came from the National Computing Centre (NCC), and later a group formed from British industry, to ensure that the Code was applicable and practical from a user's point of view. The document was originally published as British Standards guidance document PD 0003: A Code of Practice for Information Security Management. After more input was received from private sector organizations, the document was reintroduced as British Standard BS7799:1995. After two revisions in 1997 and 1999, BS7799 was proposed as an ISO standard. Though the first revisions were defeated, it was eventually adopted by the ISO after an international ballot closed in August 2000 and published with minor amendments as ISO/IEC 17799:2000 on December 1, 2000. A new version, ISO 17799:2005, was published in 2005. In 2007, this version was renamed as 27002:2005 and incorporated into the 27000 series. The most significant difference between the 17799 series and the 27000 series is an optional certification process. Organizations ISMS may be certified compliant with ISO/IEC 27001 by a number of Accredited Registrars worldwide.

In October 2013, ISO 27002:2005 was replaced with ISO 27002:2013. Two categories were added: Cryptography and Supplier Relationships. The Operations and Communications domain was split into two separate categories. Most importantly, a decision was made to remove the risk assessment guidance because it was a subset of ISO 27005, which specifically addresses information security risk management, including risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring, and risk review. More information about the ISO can be found at www.iso.org.

Can the ISO Standards and NIST Publications Be Used to Build a Framework?

The ISO 27002:2013 Code of Practice is a comprehensive set of information security recommendations comprising best practices in information security. It is intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce as well as to be used by large, medium, and small organizations. The term *organization* is used throughout this standard to mean both commercial and nonprofit organizations such as public sector and government agencies. 27002:2013 does not mandate specific controls but leaves it to the organization to select and implement controls that suit them, using a risk-assessment process to identify the most appropriate controls for their specific requirements. The recommended practices are organized into the following "domains" or categories:

- Information Security Policies
- Organization of Information Security
- Human Resources Security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security

- Operations Security
- Communications Security
- Systems Acquisition, Development, and Maintenance
- Supplier Relationships
- Information Security Incident Management
- Business Continuity Management
- Compliance Management

We will be using both the ISO 27002:2013 Code of Practice and the NIST guidance as a framework for developing procedures and policies. Using this framework will allow us to organize our approach to developing policies; it provides a structure for development and a method of grouping similar policies. The first step is to become familiar with the goals and intent of each of the security domains (or categories). In subsequent chapters, we examine each domain in depth, evaluate security practices, and develop policy.

Information Security Policies (ISO 27002:2013 Section 5)

The Information Security Policies domain focuses on information security policy requirements and the need to align policy with organizational objectives. The domain stresses the importance of management participation and support. This domain is covered in Chapter 4, "Governance and Risk Management."

The corresponding NIST Special Publications are as follows:

- SP 800-12: An Introduction to Computer Security: The NIST Handbook
- SP 800-100: Information Security Handbook: A Guide for Managers

Organization of Information Security (ISO 27002:2013 Section 6)

The Organization of Information Security domain focuses on establishing and supporting a management structure to implement and manage information security within, across, and outside the organization. Inward-facing governance concentrates on employee and stakeholder relationships. Outward-facing governance concentrates on third-party relationships. Third parties include vendors, trading partners, customers, and service providers. This domain is covered in Chapter 4.

The corresponding NIST Special Publications are as follows:

- SP 800-12: An Introduction to Computer Security: The NIST Handbook
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-100: Information Security Handbook: A Guide for Managers

Human Resources Security Management (ISO 27002:2013 Section 7)

The Human Resources Security Management domain focuses on integrating security into the employee lifecycle, agreements, and training. Human nature is to be trusting. This domain reminds us that there are both good and bad people and that we need to keep our eyes wide open. This domain is covered in Chapter 6, "Human Resources Security."

The corresponding NIST Special Publications are as follows:

- SP 800-12: An Introduction to Computer Security—The NIST Handbook
- SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model
- SP 800-50: Building an Information Technology Security Awareness and Training Program
- SP 800-100: Information Security Handbook: A Guide for Managers

Asset Management (ISO 27002:2013 Section 8)

The Asset Management domain focuses on developing classification schema, assigning classification levels, and maintaining accurate inventories of data and devices. The importance of documented handling standards to protect information is stressed. This domain is covered in Chapter 5, "Asset Management."

The corresponding NIST Special Publications are as follows:

- SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories (two volumes)
- SP 800-88: Guidelines for Media Sanitization

Access Control (ISO 27002:2013 Section 9)

The Access Control domain focuses on managing authorized access and preventing unauthorized access to information systems. This domain extends to remote locations, home offices, and mobile access. This domain is covered in Chapter 9, "Access Control Management."

The corresponding NIST Special Publications are as follows:

- SP 800-41, R1: Guidelines on Firewalls and Firewall Policy
- SP 800-46, R1: Guide to Enterprise Telework and Remote Access Security
- SP 800-63: Electronic Authentication Guidance
- SP 800-77: Guide to IPsec VPNs
- SP 800-113: Guide to SSL VPNs
- SP 880-114: User's Guide to Securing External Devices for Telework and Remote Access
- SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)

Cryptography (ISO 27002:2013 Section 10)

The Cryptography domain was added in the 2013 update. The domain focuses on proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. Special attention is paid to key management. This domain is included in Chapter 10, "Information Systems Acquisition, Development, and Maintenance."

The corresponding NIST Special Publications are as follows:

- 800-57: Recommendations for Key Management—Part 1: General (Revision 3)
- 800-57: Recommendations for Key Management—Part 2: Best Practices for Key Management Organization
- 800-57: Recommendations for Key Management—Part 3: Application-Specific Key Management Guidance
- 800-64: Security Considerations in the System Development Life Cycle
- 800-111: Guide to Storage Encryption Technologies for End User Devices

Physical and Environmental Security (ISO 27002:2013 Section 11)

The Physical and Environmental Security domain focuses on designing and maintaining a secure physical environment to prevent unauthorized access, damage, and interference to business premises. Special attention is paid to disposal and destruction. This domain is covered in Chapter 7, "Physical and Environmental Security."

The corresponding NIST Special Publications are as follows:

- SP 800-12: An Introduction to Computer Security—The NIST Handbook
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-88: Guidelines for Media Sanitization
- SP 800-100: Information Security Handbook: A Guide for Managers

Operations Security (ISO 27002:2013 Section 12)

The Operations Security domain focuses on data center operations, integrity of operations, vulnerability management, protection against data loss, and evidence-based logging. This domain is covered in Chapter 8, "Communications and Operations Security."

The corresponding NIST Special Publications are as follows:

- SP 800-40: Creating a Patch and Vulnerability Management Program
- SP 800-42: Guideline on Network Security Testing
- SP 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops

- SP 800-92: Guide to Computer Security Log Management
- SP 800-100: Information Security Handbook: A Guide for Managers

Communications Security (ISO 27002:2013 Section 13)

The Communications Security domain focuses on the protection of information in transit. The domain incorporates internal and external transmission as well as Internet-based communication. This domain is covered in Chapter 8.

The corresponding NIST Special Publications are as follows:

- SP 800-45: Guidelines on Electronic Mail Security
- SP 800-92: Guide to Computer Security Log Management
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems

Information Systems Acquisition, Development, and Maintenance (ISO 27002:2013 Section 14)

The Information Systems Acquisition, Development, and Maintenance domain focuses on the security requirements of information systems, applications, and code from conception to destruction. This sequence is referred to as the systems development lifecycle. This domain is covered in Chapter 10.

Here's the corresponding NIST Special Publication:

- SP 800-23: Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Supplier Relationships (ISO 27002:2013 Section 15)

The Supplier Relationship domain was added in the 2013 update. The domain focuses on service delivery, third-party security requirements, contractual obligations, and oversight. This domain is included in Chapter 8.

There is no corresponding NIST Special Publication.

Information Security Incident Management (ISO 27002:2013 Section 16)

The Information Security Incident Management domain focuses on a consistent and effective approach to the management of information security incidents, including detection, reporting, response, escalation, and forensic practices. This domain is covered in Chapter 11, "Information Security Incident Management."

The corresponding NIST Special Publications are as follows:

- SP 800-61: Computer Security Incident Handling Guide
- SP 800-83: Guide to Malware Incident Prevention and Handling
- SP 800-86: Guide to Integrating Forensic Techniques into Incident Response

Business Continuity (ISO 27002:2013 Section 17)

The Business Continuity Management domain focuses on availability and the secure provision essential services during a disruption of normal operating conditions. ISO 22301 provides a framework to plan, establish, implement, operate, monitor, review, maintain, and continually improve a business continuity management system (BCMS). This domain is covered in Chapter 12, "Business Continuity Management."

The corresponding NIST Special Publications are as follows:

- SP 800-34: Contingency Planning Guide for Information Technology System, Revision 1
- SP 800-84: Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities

Compliance Management (ISO 2700:2013 Section 18)

The Compliance Management domain focuses on conformance with internal policy; local, national, and international criminal and civil laws; regulatory or contractual obligations; intellectual property rights (IPR); and copyrights. This domain relates to Part III, "Regulatory Compliance" (Chapters 13, 14, and 15).

The corresponding NIST Special Publications are as follows:

- SP 800-60: Guide for Mapping Types of Information and Information Systems to Security
- SP Categories: Volume 1: Guide, Volume 2: Appendices
- SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Too Many Domains?

As with policies, for an information security program to be effective, it must be meaningful and relevant as well as appropriate to the size and complexity of the organization. Not all organizations will need all the policies referenced in the ISO 27002 Code of Practice. The key is to understand what domains are applicable to a given environment and then develop, adopt, and implement the controls and polices that make sense for the organization. Remember, policies must support, not hinder, the mission and goals of an organization.

Section 4.1 of the 27002:2013 Code of Practice document informs us that the order of the domains does not imply their importance, nor are they listed in priority order. As such, this book takes the liberty of reordering the sections and, where applicable, combining domains. Starting with Chapter 4 and continuing through Chapter 12, we map the security objectives of each domain to realistic, relevant, and usable practices and policies. We define goals and objectives, explore in detail relevant security issues, and discuss the applicability of the standard.

NOTE

Within each chapter, you will find "In Practice" sidebars that contain relevant policy statements. Each policy statement is preceded by a synopsis. The synopsis is included only as explanatory text and would not normally be included in a policy document. At the end of the book, you will find a comprehensive information security policy document that includes all the policy statements as well as the supporting policy elements discussed in Chapter 2, "Policy Elements and Style."

Summary

Ensuring confidentiality, integrity, and availability is the unifying principle of every information security program. Collectively referred to as the ***CIA triad*** or ***CIA security model***, each attribute represents a fundamental objective and corresponding action related to the protection of information, processes, or systems. ***Confidentiality*** is protection from unauthorized access or disclosure. ***Integrity*** is protection from manipulation. ***Availability*** is protection from denial of service (DOS). In support of the CIA triad are the security principles known as the ***Five A's***: accountability, assurance, authentication, accounting, and authorization.

An ***information owner*** is one who has been assigned the authority and responsibility for ensuring that information and related systems are protected from creation through destruction. This includes making decisions on information classification, safeguards, and controls. ***Information custodians*** are those responsible for implementing, maintaining, and monitoring the safeguards based on decisions made by information owners. Cohesive decision making requires a framework.

A ***security framework*** is a collective term given to guidance on topics related to information systems security, predominantly regarding the planning, implementing, managing, and auditing of overall information security practices. The ***International Organization for Standardization*** (ISO) has published a technology-neutral Code of Standards for Information Security known as the ISO/IEC 27002:2013. This standard has been internationally adopted by both private and public organizations of all sizes. ISO 27002:2013 is divided into 14 domains. Each of these categories has a control objective, compliance requirements, and recommended policy components. The United States ***National Institute of Standards and Technology*** (NIST) has a number of Special Publications that complement the ISO Code of Practice. The publications provide in-depth research, recommendations, and guidance that can be applied to security domains and specific technologies. In this book, we use both to build our information security policy and program.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following are the three principles in the CIA triad?

   A. Confidence, integration, availability

   B. Consistency, integrity, authentication

   C. Confidentiality, integrity, availability

   D. Confidentiality, integrity, awareness

2. Which of the following is an example of acting upon the goal of integrity?

   A. Ensuing that only authorized users can access data

   B. Ensuring that systems have 99.9% uptime

   C. Ensuring that all modifications go through a change-control process

   D. Ensuring that changes can be traced back to the editor

3. Which of the following is a control that relates to availability?

   A. Disaster recovery site

   B. Firewall

   C. Training

   D. Encryption

4. Which of the following is an objective of confidentiality?

   A. Protection from unauthorized access

   B. Protection from manipulation

   C. Protection from denial of service

   D. Protection from authorized access

5. As it pertains to information security, assurance is ____________________________.

   A. the process of tracing actions to their source

   B. the processes, policies, and controls used to develop confidence that security measures are working as intended

   C. the positive identification of the person or system seeking access to secured information or systems

   D. the logging of access and usage of information resources

6. Which of the following terms best describes the granting of users and systems a predetermined level of access to information resources?

   A. Availability

   B. Accountability

   C. Assurance

   D. Authorization

7. Which of the following statements identify threats to availability? (Select all that apply.)

   A. Loss of processing capabilities due to natural disaster or human error

   B. Loss of confidentiality due to unauthorized access

   C. Loss of personnel due to accident

   D. Loss of reputation from unauthorized event

8. Which of the following terms best describes the logging of access and usage of information resources?

   A. Accountability
   B. Acceptance
   C. Accounting
   D. Actuality

9. Which of the following combination of terms best describes the Five A's of information security?

   A. Awareness, acceptance, availability, accountability, authentication
   B. Awareness, acceptance, authority, authentication, availability
   C. Accountability, assurance, authorization, authentication, accounting
   D. Acceptance, authentication, availability, assurance, accounting

10. An information owner is responsible for ______________________.

   A. maintaining the systems that store, process, and transmit information
   B. protecting the information and the business results derived from use of that information
   C. protecting the people and processes used to access digital information
   D. none of the above

11. Which of the following terms best describes ISO?

   A. Internal Standards Organization
   B. International Organization for Standardization
   C. International Standards Organization
   D. Internal Organization of Systemization

12. Which of the following statements best describes opportunistic crime?

   A. Crime that is well-planned
   B. Crime that is targeted
   C. Crime that takes advantage of an identified weakness
   D. Crime that is quick and easy

13. Which of the following terms best describes the motivation for hactivism?

   A. Financial
   B. Political
   C. Personal
   E. Fun

14. The greater the criminal work factor, the _____

    A. more time it takes

    B. more profitable the crime is

    C. better chance of success

    D. less chance of getting caught

15. Which of the following terms best describes an attack whose purpose is to make a machine or network resource unavailable for its intended use?

    A. Man-in-the-middle

    B. Data breach

    C. Denial of service

    D. SQL injection

16. Information custodians are responsible for _____

    A. writing policy

    B. classifying data

    C. approving budgets

    D. implementing safeguards

17. The National Institute of Standards and Technology (NIST) is a(n) ______

    A. international organization

    B. privately funded organization

    C. U.S. government agency

    D. European Union agency

18. The Internal Organization for Standardization (ISO) is _____

    A. a nongovernmental organization

    B. an international organization

    C. headquartered in Geneva

    D. all of the above

19. The current ISO family of standards that relates to information security is _______________.

    A. BS 7799:1995

    B. ISO 17799:2006

    C. ISO/IEC 27000

    D. None of the above

20. Which of the following terms best describes the security domain that relates to determining the appropriate safeguards as it relates to the likelihood of a threat to an organization?

    A. Security policy
    B. Access control
    C. Compliance
    D. Risk assessment

21. Which of the following terms best describes the security domain that relates to how data is classified and valued?

    A. Security policy
    B. Asset management
    C. Compliance
    D. Access control

22. Which of the following terms best describes the security domain that includes HVAC, fire suppression, and secure offices?

    A. Operations
    B. Communications
    C. Risk assessment
    D. Physical and environmental controls

23. Which of the following terms best describes the security domain that aligns most closely with the objective of confidentiality?

    A. Access control
    B. Compliance
    C. Incident management
    D. Business continuity

24. The primary objective of the __________ domain is to ensure conformance with GLBA, HIPAA, PCI/DSS, FERPA, and FISMA.

    A. Security Policy
    B. Compliance
    C. Access Control
    D. Contract and Regulatory

25. Processes that include responding to a malware infection, conducting forensics investigations, and reporting breaches are included in the _____________ domain.

    A. Security Policy
    B. Operations and Communications
    C. Incident Management
    D. Business Continuity Management

26. Which of the following terms best describes a synonym for business continuity?

    A. Authorization
    B. Authentication
    C. Availability
    D. Accountability

27. The ____________ can be held legally responsible for the safeguarding of legally protected information.

    A. information user
    B. information owner
    C. information custodian
    D. information author

28. Personnel screening, acceptable use, confidentiality agreements, and training are controls that relate to the ______________ domain.

    A. Operations and Communications
    B. Security Policy
    C. Human Resources
    D. Legal and Compliance

29. Defining organizational roles, responsibilities, and authority relate to the __________ domain.

    A. Operations and Communications
    B. Security Policy
    C. Governance
    D. Legal and Compliance

30. Which of the following security objectives is most important to an organization?

    A. Confidentiality
    B. Integrity
    C. Availability
    D. The answer may vary from organization to organization.

EXERCISES

EXERCISE 3.1: Understanding CIA

1. Define the security term “confidentiality.” Provide an example of a business situation where confidentiality is required.
2. Define the security term “integrity.” Provide an example of a business situation in which the loss of integrity could result in significant harm.
3. Define the security term “availability.” Provide an example of a business situation in which availability is more important than confidentiality.

EXERCISE 3.2: Understanding Opportunistic Cybercrime

1. Define what is meant by an “opportunistic” crime.
2. Provide an example.
3. Locate (online) a copy of the most recent Verizon Data Breach Incident Report. What percentage of cybercrimes are considered “opportunistic”?

EXERCISE 3.3: Understanding Hacktivism or DDoS

1. Find a recent news article relating to either hacktivism or a distributed denial of service (DDoS) attack.
2. Summarize the attack.
3. Explain why the attacker was successful (or not).

EXERCISE 3.4: Understanding NIST and ISO

1. At their respective websites, read the Mission and About sections of both the ISO (www.iso.org) and the NIST Computer Security Resource Center (http://csrc.nist.gov/). Describe the similarities and differences between the organizations.
2. Which do you think is more influential, and why?

EXERCISE 3.5: Understanding ISO 27002

1. Choose one of the ISO 27002:2013 categories and explain why this domain is of particular interest to you.
2. ISO 27002 Supplier Relationships (Section 15) was added in the 2013 version. Why do you think this section was added?
3. 27002:2013 does not mandate specific controls but leaves it to the organization to select and implement controls that suit them. NIST Special Publications provide specific guidance. In your opinion, which approach is more useful?

PROJECTS

PROJECT 3.1: Conducting a CIA Model Survey

1. Survey ten people about the importance of the CIA model to them. Use the following table as a template. Ask them to name three types of data they have on their phone or tablet. For each data type, ask which is more important—that the information on their device be kept confidential (C), be correct (I), or be available (A).

#	Participant Name	Device Type	Data Type 1	CIA	Data Type 2	CIA	Data Type 3	CIA
1.	Sue Smith	iPhone	Phone numbers	I	Pictures	A	Text messages	C
2.								
3.								

2. Summarize the responses.
3. Are the responses inline with your expectations? Why or why not?

PROJECT 3.2: Preparing a Report Based on the NIST Special Publications 800 Series Directory

1. Locate the NIST Special Publications 800 Series directory.
2. Read through the list of documents. Choose one that interests you and read it.
3. Prepare a report that addresses the following:
   a. Why you chose this topic
   b. What audience the document was written for
   c. Why this document would be applicable to other audiences
   d. The various sections of the document
   e. Whether the document addresses confidentiality, integrity, or availability

PROJECT 3.3: Preparing a Report on ISO 27001 Certification

1. Research how many organizations are currently ISO 27001 certified.
2. Prepare a report on how an organization achieves ISO 27001 certification.

Case Study

Policy Writing Approach

Regional Bank has been growly rapidly. In the past two years, it has acquired six smaller financial institutions. The long-term strategic plan is for the bank to keep growing and to "go public" within the next three to five years. FDIC regulators have told management that they will not approve any additional acquisitions until the bank strengthens its information security program. The regulators commented that Regional Bank's information security policy is confusing, lacking in structure, and filled with discrepancies. You have been tasked with "fixing" the problems with the policy document.

1. Consider the following questions: Where do you begin this project? Would you use any material from the original document? What other materials should you request? Would you want to interview the author of the original policy? Who else would you interview? Should the bank work toward ISO certification? Which ISO 27002:2013 domains and sections would you include? What other criteria should you consider?
2. Create a project plan of how you would approach this project.

References

Regulations Cited

"Federal Code 44 U.S.C., Sec. 3542," accessed on 06/2013, http://uscode.house.gov/download/pls/44C35.txt.

"Federal Information Security Management Act (FISMA)," accessed on 06/2013, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

"Public Law 107 – 347 – E-Government Act of 2002," official website of the U.S. Government Printing Office, accessed on 06/2013, www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html.

ISO Research

"International Standard ISO/IEC 27001," First Edition 2005-10-15, published by the ISO, Switzerland.

"International Standard ISO/IEC 27000," Second Edition 2012-12-01, published by the ISO, Switzerland.

"International Standard ISO/IEC 27002:2013," Second Edition 2013-10-01, published by the ISO, Switzerland.

"About ISO," official website of the International Organization for Standardization (ISO), accessed on 06/2013, www.iso.org/iso/home/about.htm.

"A Short History of the ISO 27000 Standards: Official," The ISO 27000 Directory, accessed on 06/2013, www.27000.org/thepast.htm.

"An Introduction to ISO 27001, ISO 27002, … ISO 27008," The ISO 27000 Directory, accessed on 06/2013, www.27000.org/index.htm.

"The ISO/IEC 27000 Family of Information Security Standards," IT Governance, accessed on 06/2013, www.itgovernance.co.uk/iso27000-family.aspx.

"ISO/IEC 27000 Series," Wikipedia, accessed on 06/2013, http://en.wikipedia.org/wiki/ISO/IEC_27000-series.

NIST Research

"NIST General Information," official website of the National Institute of Standards and Technology, accessed on 06/2013, www.nist.gov/public_affairs/general_information.cfm.

"NIST Computer Security Division," official website of the NIST Computer Security Resource Center, accessed on 06/2013, http://csrc.nist.gov/.

"Federal Information Processing Standards (FIPS) Publications," official website of the NIST Computer Security Resource Center, accessed on 06/2013, http://csrc.nist.gov/publications/PubsFIPS.html.

"Special Publications (800 Series) Directory," official website of the NIST Computer Security Resource Center, accessed on 06/2013, http://csrc.nist.gov/publications/PubsSPs.html.

"Special Publications (800 Series) Directory by Legal requirement," official website of the NIST Computer Security Resource Center, accessed on 06/2013, http://csrc.nist.gov/publications/PubByLR.html.

Other References

"Distributed Denial of Service Attack (DDoS)," Security Search, accessed on 06/2013, http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

"Hacktivism," Wikipedia, accessed on 06/2013, http://en.wikipedia.org/wiki/index.html?curid=162600.

Kuligowski, Christine, "Comparison of IT Security Standards (2009)," accessed on 06/2013, www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf.

Metac0m, "What Is Hactivism? 2.0," published by *The Hacktivist*, December 2003, accessed on 06/2013, www.thehacktivist.com/whatishacktivism.pdf.

Poulen, K. and Zetter, K. "U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe," *Wired Magazine*, accessed on 06/2013, http://www.wired.com/threatlevel/2010/06/leak/.

"What Is WikiLeaks," WikiLeaks, accessed on 06/2013, http://wikileaks.org/About.html.

"WikiLeaks Fast Facts," CNN, accessed on 06/01/2013, www.cnn.com/2013/06/03/world/wikileaks-fast-facts/.

Chapter 4

Governance and Risk Management

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Explain the importance of strategic alignment.
- Know how to manage information security policies.
- Describe information security–related roles and responsibilities.
- Identify the components of risk management.
- Create polices related to information security policy, governance, and risk management.

Information Security Policies (ISO 27002:2013 Section 5) and Organization of Information Security (ISO 27002:2013 Section 6) are closely related, so we address both domains in this chapter. The Information Security Policies domain focuses on information security policy requirements and the need to align policy with organizational objectives. The Organization of Information Security domain focuses on the governance structure necessary to implement and manage information security policy operations, across and outside of the organization. Included in this chapter is a discussion of risk management because it is a fundamental aspect of governance, decision making, and policy. Risk management is important enough that it warrants two sets of standards: ISO/IEC 27005 and ISO/IEC 31000.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 5 of ISO 27002:2013 is titled "Information Security Policies." This domain addresses policy development and authorization. Section 6 of ISO 27002:2013 is titled "Organization of Information Security." This domain addresses information security governance as well as enterprise roles and responsibilities. Risk management principles, risk assessment techniques, and information security risk management systems are described in ISO 27005:2005 and the ISO 31000 series.

Corresponding NIST guidance is provided in the following documents:

- SP 800-12: An Introduction to Computer Security: The NIST Handbook
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-30: Risk Management Guide for Information Technology Systems
- SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View
- SP 800-100: Information Security Handbook: A Guide for Managers

Understanding Information Security Policies

Information security policies, standards, procedures, and plans exist for one reason—to protect the organization and, by extension, its constituents from harm. The lesson of the Information Security Policies domain is threefold:

- Information security directives should be codified in a written policy document.
- It is important that management participate in policy development and visibly support the policy.
- The necessity of strategically aligning information security with business requirements and relevant laws and regulations.

Internationally recognized standard security standards such as the ISO 27002:2013 can provide a framework, but ultimately each organization must construct its own security strategy and policy taking into consideration organizational objectives and regulatory requirements.

What Is Meant by Strategic Alignment?

The two approaches to information security are parallel and integrated. A ***parallel approach*** silos information security, assigns responsibility for *being secure* to the IT department, views compliance as discretionary, and has little or no organizational accountability. An ***integrated approach*** recognizes that security and success are intertwined. When strategically aligned, security functions as a business enabler that adds value. Security is an expected topic of discussion among decision makers and is given the same level of respect as other fundamental drivers and influencing elements of the business. This doesn't happen magically. It requires leadership that recognizes the value of information security, invests in people and processes, encourages discussion and debate, and treats security in the same fashion as every other business requirement. It also requires that information security professionals recognize that the true value of information security is protecting the business from harm and achieving organizational objectives. Visible management support coupled with written policy formalizes and communicates the organizational commitment to information security.

Regulatory Requirements

In an effort to protect the citizens of the United States, legislators recognized the importance of written information security policies. Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Family Educational Rights and Privacy Act (FERPA), and the Federal Information Systems Management Act (FISMA) all require covered entities to have in place written policies and procedures that protect their information assets. They also require the policies to be reviewed on a regular basis. Each of these legislative acts better secured each person's private information and the governance to reduce fraudulent reporting of corporate earnings.

Many organizations find that they are subject to more than one set of regulations. For example, publicly traded banks are subject to both GLBA and SOX requirements, whereas medical billing companies find themselves subject to both HIPAA and GLBA. Organizations that try to write their policies to match federal state regulations find the task daunting. Fortunately, the regulations published to date have enough in common that a well-written set of information security policies based on a framework such as the ISO 27002 can be mapped to multiple regulatory requirements. Policy administrative notations will often include a cross-reference to specific regulatory requirements.

User Versions of Information Security Policies

Information security policies are governance statements written with the intent of directing the organization. Correctly written, policies can also be used as teaching documents that influence behavior. An Acceptable Use Policy document and corresponding agreement should be developed specifically for distribution to the user community. The Acceptable Use Policy should include only pertinent information and, as appropriate, explanations and examples. The accompanying agreement requires users to acknowledge that they understand their responsibilities and affirm their individual commitment.

Vendor Versions of Information Security Policies

As we will discuss in Chapter 8, "Communications and Operations Security," companies can outsource work but not responsibility or liability. Vendors or business partners (often referred to as "third parties") that store, process, transmit, or access information assets should be required to have controls that meet or, in some cases, exceed organizational requirements. One of the most efficient ways to evaluate vendor security is to provide them with a vendor version of organizational security policies and require them to attest to their compliance. The vendor version should only contain policies that are applicable to third parties and should be sanitized as to not disclose any confidential information.

Client Synopsis of Information Security Policies

In this context, *client* refers to companies to which the organization provides services. A synopsis of the information security policy should be available upon request to clients. As applicable to the client base, the synopsis could be expanded to incorporate incident response and business continuity procedures, notifications, and regulatory cross-references. The synopsis should not disclose confidential business information unless the recipients are required to sign a non-disclosure agreement.

In Practice

Information Security Policy

Synopsis: The organization is required to have a written information security policy and supporting documents.

Policy Statement:

- The company must have written information security policies.
- Executive management is responsible for establishing the mandate and general objectives of the information security policy.
- The policies must support organizational objectives.
- The policies must comply with relevant statutory, regulatory, and contractual requirements.
- The policies must be communicated to all relevant parties both within and external to the company.
- As applicable, standards, guidelines, plans, and procedures must be developed to support the implementation of policy objectives and requirements.
- For the purpose of educating the workforce, user-level documents will be derived from the information security policy including but not limited to Acceptable Use Policy, Acceptable Use Agreement, and Information Handling Instructions.
- Any information security policy distributed outside the organization must be sanitized.
- All documentation will be retained for a period of six years from the last effective date.

FYI: Policy Hierarchy Refresher

- ***Guiding principles*** are the fundamental philosophy or beliefs of an organization and reflect the kind of company an organization seeks to be. The policy hierarchy represents the implementation of guiding principles.
- ***Policies*** are directives that codify organizational requirements.
- ***Standards*** are implementation specifications.
- ***Baselines*** are an aggregate of minimum implementation standards and security controls for a specific category or grouping.
- ***Guidelines*** are suggested actions or recommendations.
- ***Procedures*** are instructions.
- ***Plans*** are strategic and tactical guidance used to execute an initiative or respond to a situation, within a certain timeframe, usually with defined stages and with designated resources.

Who Authorizes Information Security Policy?

A policy is a reflection of the organization's commitment, direction, and approach. Information security policies should be authorized by executive management. Depending on the size, legal structure, and/or regulatory requirements of the organization, executive management may be defined as owners, directors, or executive officers.

Because executive management is responsible for and can be held legally liable for the protection of information assets, it is incumbent upon those in leadership positions to remain invested in the proper execution of the policy as well as the activities of oversight that ensure it. The National Association of Corporate Directors (NACD), the leading membership organization for Boards and Directors in the U.S., recommends four essential practices:

- Place information security on the Board's agenda.
- Identify information security leaders, hold them accountable, and ensure support for them.
- Ensure the effectiveness of the corporation's information security policy through review and approval.
- Assign information security to a key committee and ensure adequate support for that committee.

Policies should be reviewed at planned intervals to ensure their continuing suitability, adequacy, and effectiveness.

FYI: Director's Liability and Duty of Care

In tort law, duty of care is a legal standard applied to directors and officers of a corporation. In 1996, the shareholders of Caremark International, Inc., brought a derivative action, alleging that the Board of Directors breached their duty of care by failing to put in place adequate internal control systems. In response, the Delaware court defined a multifactor test designed to determine when duty of care is breached:

- The directors knew or should have known that violations of the law were occurring, and
- The directors took no steps in a good faith effort to prevent or remedy the situation, and
- Such failure proximately resulted in the losses complained of.

According to the firm of Orrick, Herrington and Sutcliffe, LLP, "in short, as long as a director acts in good faith, as long as she exercises proper due care and does not exhibit gross negligence, she cannot be held liable for failing to anticipate or prevent a cyber attack. However, if a plaintiff can show that a director failed to act in the face of a known duty to act, thereby demonstrating a conscious disregard for [her] responsibilities, it could give rise to a claim for breach of fiduciary duty."

Revising Information Security Policies: Change Drivers

Because organizations change over time, policies need to be revisited. ***Change drivers*** are events that modify how a company does business. Change drivers can be demographic, economic, technological, and regulatory or personnel related. Examples of change drivers include company acquisition, new products, services or technology, regulatory updates, entering into a contractual obligation, and entering a new market. Change can introduce new vulnerabilities and risks. Change drivers should trigger internal assessments and ultimately a review of policies. Policies should be updated accordingly and subject to reauthorization.

Evaluating Information Security Polices

Directors and executive management have a fiduciary obligation to manage the company in a responsible manner. It is important that they be able to accurately gauge adherence to policy directives, the effectiveness of information security policies, and the maturity of the information security program. Standardized methodologies such as audits and maturity models can be used as evaluation and reporting mechanisms. Organizations may choose to conduct these evaluations using in-house personnel or engage independent third parties. The decision criteria include the size and complexity of the organization, regulatory requirements, available expertise, and segregation of duties. To be considered ***independent***, assessors should not be responsible for, benefit from, or have in any way influenced the design, installation, maintenance, and operation of the target, or the policies and procedures that guide its operation.

Audit

An ***information security audit*** is a systematic, evidence-based evaluation of how well the organization conforms to established criteria such as Board-approved policies, regulatory requirements, and internationally recognized standards such as the ISO 27000 series. Audit procedures include interviews, observation, tracing documents to management policies, review of practices, review of documents, and tracing data to source documents. An ***audit report*** is a formal opinion (or disclaimer) of the audit team based on predefined scope and criteria. Audit reports generally include a description of the work performed, any inherent limitations of the work, detailed findings, and recommendations.

FYI: Certified Information Security Auditor (CISA)

The CISA certification is granted by ISACA (previously known as the Information Systems Audit and Control Association) to professionals who have demonstrated a high degree of audit-related knowledge and have verifiable work experience. The CISA certification is well respected across the globe, and the credibility of its continuing professional education (CPE) program ensures that CISA-certified professionals maintain their skill set. The American National Standards Institute (ANSI) accredited the CISA certification program under ISO/IEC 17024:2003: General Requirements for Bodies Operating Certification Systems of Persons. For more information about ISACA certification, visit www.isaca.org.

Capability Maturity Model (CMM)

A ***capability maturity model (CMM)*** is used to evaluate and document process maturity for a given area. The term *maturity* relates to the degree of formality and structure, ranging from ad hoc to optimized processes. Funded by the United States Air Force, the CMM was developed in the mid-1980s at the Carnegie Mellon University Software Engineering Institute. The objective was to create a model for the military to use to evaluate software development. It has since been adopted for subjects as diverse as information security, software engineering, systems engineering, project management, risk management, system acquisition, information technology (IT) services, and personnel management. It is sometimes combined with other methodologies such as ISO 9001, Six Sigma, Extreme Programming (XP), and DMAIC.

As documented in Table 4.1, a variation of the CMM can be used to evaluate enterprise information security maturity. Contributors to the application of the model should possess intimate knowledge of the organization and expertise in the subject area.

TABLE 4.1 Capability Maturity Model (CMM) Scale

Level	State	Description
0	Nonexistent	The organization is unaware of the need for policies or processes.
1	Ad-hoc	There are no documented policies or processes; there is sporadic activity.
2	Repeatable	Policies and processes are not fully documented; however, the activities occur on a regular basis.
3	Defined process	Policies and processes are documented and standardized; there is an active commitment to implementation.
4	Managed	Policies and processes are well defined, implemented, measured, and tested.
5	Optimized	Policies and process are well understood and have been fully integrated into the organizational culture.

As Figure 4.1 illustrates, the result is easily expressed in a graphic format and succinctly conveys the state of the information security program on a per-domain basis. The challenge with any scale-based model is that sometimes the assessment falls in between levels, in which case it is perfectly appropriate to use gradations (such as 3.5). This is an effective mechanism for reporting to those responsible for oversight, such as the Board of Directors or executive management. Process improvement objectives are a natural outcome of a CMM assessment.

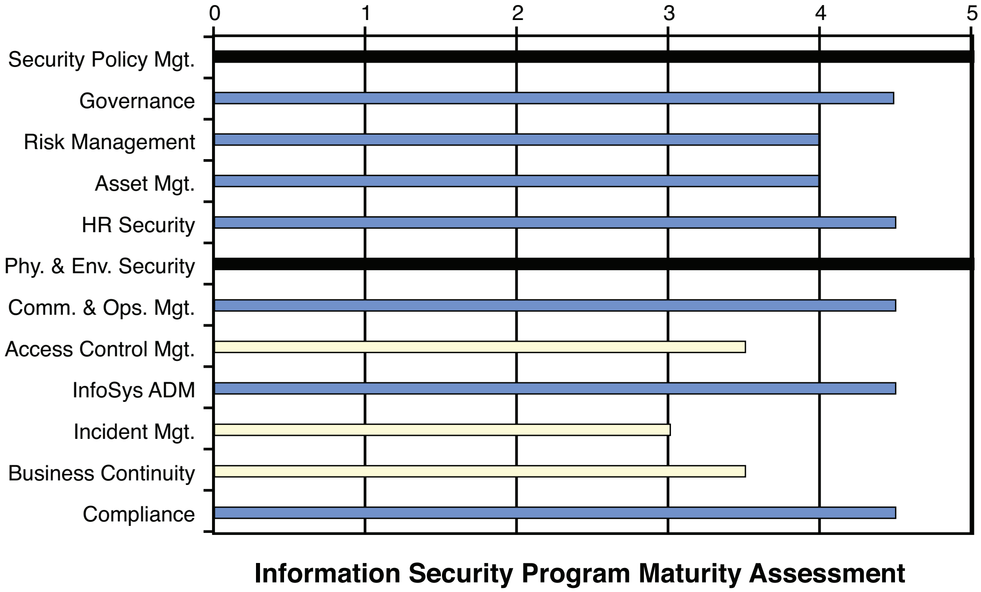


FIGURE 4.1 Capability maturity model (CMM) assessment.

In Practice

Information Security Policy Authorization and Oversight Policy

Synopsis: Information security policies must be authorized by the Board of Directors. The relevancy and the effectiveness of the policy must be reviewed annually.

Policy Statement:

- The Board of Directors must authorize the information security policy.
- An annual review of the information security policy must be conducted.
- The Chief Information Security Officer (CISO) is responsible for managing the review process.
- Changes to the policy must be presented to and approved by a majority of the Board of Directors.
- The Chief Operating Officer (COO) and the CISO will jointly present an annual report to the Board of Directors that provides them the information necessary to measure the organizations' adherence to the information security policy objectives and the maturity of the information security program.
- When in-house knowledge is not sufficient to review or audit aspects of the information security policy, or if circumstances dictate independence, third-party professionals must be engaged.

Information Security Governance

Governance is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors. The ISO 27002:2013 Organization of Information Security domain objective is "to establish a management framework to initiate and control the implementation and operation of information security within the organization." This domain requires organizations to decide who is responsible for security management, the scope of their authority, and how and when it is appropriate to engage outside expertise. Julie Allen, in her seminal work "Governing for Enterprise Security," passionately articulated the importance of governance as applied to information security:

"Governing for enterprise security means viewing adequate security as a non-negotiable requirement of being in business. If an organization's management—including boards of directors, senior executives and all managers—does not establish and reinforce the business need for effective enterprise security, the organization's desired state of security will not be articulated, achieved or sustained. To achieve a sustainable capability, organizations must make enterprise security the responsibility of leaders at a governance level, not of other organizational roles that lack the authority, accountability, and resources to act and enforce compliance."

The Board of Directors (or organizational equivalent) is generally the authoritative policy-making body and responsible for overseeing the development, implementation, and maintenance of the information security program. The use of the term "oversee" is meant to convey the Board's conventional supervisory role, leaving day-to-day responsibilities to management. Executive management should be tasked with providing support and resources for proper program development, administration, and maintenance as well as ensuring strategic alignment with organizational objectives.

What Is a Distributed Governance Model?

It is time to bury the myth that "security is an IT issue." Security is not an isolated discipline and should not be siloed. Designing and maintaining a secure environment that supports the mission of the organization requires enterprise-wide input, decision making, and commitment. The foundation of a distributed governance model is the principle that stewardship is an organizational responsibility. Effective security requires the active involvement, cooperation, and collaboration of stakeholders, decision makers, and the user community. Security should be given the same level of respect as other fundamental drivers and influencing elements of the business.

Chief Information Security Officer (CISO)

Even in the most security-conscious organization, someone still needs to provide expert leadership. That is the role of the CISO. As a member of the executive team, the CISO is positioned to be a leader, teacher, and security champion. The CISO coordinates and manages security efforts across the company, including IT, human resources (HR), communications, legal, facilities management, and other groups. The most successful CISOs successfully balance security, productivity, and innovation. The CISO must be an advocate for security as a business enabler while being mindful of the need to protect the organizational from unrecognized harm. They must be willing to not be the most popular person in the room. This position generally reports directly to a senior functional executive (CEO, COO, CFO, General Counsel) and should have an unfiltered communication channel to the Board of Directors.

In smaller organizations, this function is often vested in the non-executive-level position of Information Security Officer (ISO). A source of conflict in many companies is whom the ISO should report to and if they should be a member of the IT team. It is not uncommon or completely out of the question for the position to report to the CIO. However, this chain of command can raise questions concerning adequate levels of independence. To ensure appropriate segregation of duties, the ISO should report directly to the Board or to a senior officer with sufficient independence to perform their assigned tasks. Security officers should not be assigned operational responsibilities within the IT department. They should have sufficient knowledge, background, and training, as well as a level of authority that enables them to adequately and effectively perform their assigned tasks. Security decision making should not be a singular task. Supporting the CISO or ISO should be a multidisciplinary committee that represents functional and business units.

In Practice

CISO Policy

Synopsis: To define the role of the CISO as well as the reporting structure and lines of communication.

Policy Statement:

- The COO will appoint the CISO.
- The CISO will report directly to the COO.
- At his or her discretion, the CISO may communicate directly with members of the Board of Directors.
- The CISO is responsible for managing the information security program, ensuring compliance with applicable regulations and contractual obligations, and working with business units to align information security requirements and business initiatives.
- The CISO will function as an internal consulting resource on information security issues.
- The CISO will chair the Information Security Steering Committee.
- The CISO will be a standing member of the Incident Response Team and the Continuity of Operations Team.
- Quarterly, the CISO will report to the executive management team on the overall status of the information security program. The report should discuss material matters, including such issues as risk assessment, risk management, control decisions, service provider arrangements, results of testing, security breaches or violations, and recommendations for policy changes.

Information Security Steering Committee

Creating a culture of security requires positive influences at multiple levels within an organization. Having an Information Security Steering Committee provides a forum to communicate, discuss, and debate on security requirements and business integration. Typically, members represent a cross-section of business lines or departments, including operations, risk, compliance, marketing, audit, sales, HR, and legal. In addition to providing advice and counsel, their mission is to spread the gospel of security to their colleagues, coworkers, subordinates, and business partners.

In Practice

Information Security Steering Committee Policy

Synopsis: The Information Security Steering Committee (ISC) is tasked with supporting the information security program.

Policy Statement:

- The Information Security Steering Committee serves in an advisory capacity in regards to the implementation, support, and management of the information security program, alignment with business objectives, and compliance with all applicable state and federal laws and regulations.
- The Information Security Steering Committee provides an open forum to discuss business initiatives and security requirements. Security is expected to be given the same level of respect as other fundamental drivers and influencing elements of the business.
- Standing membership will include the CISO (Chair), the COO, the Director of Information Technology, the Risk Officer, the Compliance Officer, and business unit representatives. Adjunct committee members may include but are not limited to representatives of HR, training, and marketing.
- The Information Security Steering Committee will meet on a monthly basis.

Organizational Roles and Responsibilities

In addition to the CISO and the Information Security Steering Committee, distributed throughout the organization are a variety of roles that have information security–related responsibilities. For example:

- **Compliance Officer**—Responsible for identifying all applicable information security–related statutory, regulatory, and contractual requirements.
- **Privacy Officer**—Responsible for the handling and disclosure of data as it relates to state, federal, and international law and customs.
- **Internal audit**—Responsible for measuring compliance with Board-approved policies and to ensure that controls are functioning as intended.
- **Incident response team**—Responsible for responding to and managing security-related incidents.
- **Data owners**—Responsible for defining protection requirements for the data based on classification, business need, legal, and regulatory requirements; reviewing the access controls; and monitoring and enforcing compliance with policies and standards.

- **Data custodians**—Responsible for implementing, managing, and monitoring the protection mechanisms defined by data owners and notifying the appropriate party of any suspected or known policy violations or potential endangerments.
- **Data users**—Are expected to act as agents of the security program by taking reasonable and prudent steps to protect the systems and data they have access to.

Each of these responsibilities should be documented in policies, job descriptions, or employee manuals.

Regulatory Requirements

The necessity of formally assigning information security–related roles and responsibilities cannot be overstated. The requirement has been codified in numerous standards, regulations, and contractual obligations—most notably:

- **Gramm-Leach-Bliley (GLBA) Section 314.4**: "In order to develop, implement, and maintain your information security program, you shall (a) Designate an employee or employees to coordinate your information security program."
- **HIPAA/HITECH Security Rule Section 164.308(a)**: "Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity."
- **Payment Card Industry Data Security Standard (PCI DDS) Section 12.5**: "Assign to an individual or team the following information security management responsibilities: establish, document, and distribute security policies and procedures; monitor and analyze security alerts and information, and distribute to appropriate personnel; establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations; administer user accounts, including additions, deletions, and modifications; monitor and control all access to data."
- **201 CMR 17: Standards for the Protection of Personal Information of the Residents of the Commonwealth – Section 17.0.2:** "Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to: (a) Designating one or more employees to maintain the comprehensive information security program."

Creating a culture of security requires positive influences at multiple levels within an organization. Security champions reinforce by example the message that security policies and practices are important to the organization. The regulatory requirement to assign security responsibilities is a de facto mandate to create security champions.

Information Security Risk

Three factors influence information security decision making and policy development:

- Guiding principles
- Regulatory requirements
- Risks related to achieving their business objectives.

Risk is the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction. The motivation for "taking a risk" is a favorable outcome. "Managing risk" implies that other actions are being taken to either mitigate the impact of the undesirable or unfavorable outcome and/or enhance the likelihood of a positive outcome.

For example, a venture capitalist (VC) decides to invest a million dollars in a startup company. The risk (undesirable outcome) in this case is that the company will fail and the VC will lose part or all of her investment. The motivation for taking this risk is that the company becomes wildly successful and the initial backers make a great deal of money. To influence the outcome, the VC may require a seat on the Board of Directors, demand frequent financial reports, and mentor the leadership team. Doing these things, however, does not guarantee success. ***Risk tolerance*** is how much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit—in this case, how much money the VC is willing to lose. Certainly, if the VC believed that the company was destined for failure, the investment would not be made. Conversely, if the VC determined that the likelihood of a three-million-dollar return on investment was high, she may be willing to accept the tradeoff of a potential $200,000 loss.

Is Risk Bad?

Inherently, risk is neither good nor bad. All human activity carries some risk, although the amount varies greatly. Consider this: Every time you get in a car you are risking injury or even death. You manage the risk by keeping your car in good working order, wearing a seat beat, obeying the rules of the road, not texting, not being impaired, and paying attention. Your risk tolerance is that the reward for reaching your destination outweighs the potential harm.

Risk taking can be beneficial and is often necessary for advancement. For example, entrepreneurial risk taking can pay off in innovation and progress. Ceasing to take risks would quickly wipe out experimentation, innovation, challenge, excitement, and motivation. Risk taking can, however, be detrimental when ill considered or motivated by ignorance, ideology, dysfunction, greed, or revenge. The key is to balance risk against rewards by making informed decisions and then managing the risk commensurate with organizational objectives. The process of managing risk requires organizations to assign risk-management responsibilities, establish the organizational risk appetite and tolerance, adopt a standard methodology for assessing risk, respond to risk levels, and monitor risk on an ongoing basis.

Risk Appetite and Tolerance

Risk appetite is a strategic construct and broadly defined as the amount of risk an entity is willing to accept in pursuit of its mission. Risk tolerance is tactical and specific to the target being evaluated. Risk tolerance levels can be qualitative (for example, low, elevated, severe) or quantitative (for example, dollar loss, number of customers impacted, hours of downtime). It is the responsibility of the Board of Directors and executive management to establish risk tolerance criteria, set standards for acceptable levels of risk, and disseminate this information to decision makers throughout the organization.

In Practice

Information Security Risk Management Oversight Policy

Synopsis: To assign organizational roles and responsibilities with respect to risk management activities.

Policy Statement:

- Executive management, in consultation with the Board of Directors, is responsible for determining the organizational risk appetite and risk tolerance levels.
- Executive management will communicate the above to decision makers throughout the company.
- The CISO, in consultation with the Chief Risk Officer, is responsible for determining the information security risk assessment schedule, managing the risk assessment process, certifying results, jointly preparing risk reduction recommendations with business process owners, and presenting the results to executive management.
- The Board of Directors will be apprised by the COO of risks that endanger the organization, stakeholders, employees, or customers.

What Is a Risk Assessment?

An objective of a risk assessment is to evaluate what could go wrong, the likelihood of such an event occurring, and the harm if it did. In information security, this objective is generally expressed as the process of (a) identifying the *inherent risk* based on relevant *threats*, *threat sources*, and related *vulnerabilities*; (b) determining the *impact* if the threat source was successful; and (c) calculating the *likelihood of occurrence*, taking into consideration the *control* environment in order to determine *residual* risk.

- ***Inherent risk*** is the level of risk before security measures are applied.
- A ***threat*** is a natural, environmental, or human event or situation that has the potential for causing undesirable consequences or impact. Information security focuses on the threats to confidentiality (unauthorized use or disclosure), integrity (unauthorized or accidental modification), and availability (damage or destruction).

- A ***threat source*** is either (1) intent and method targeted at the intentional exploitation of a vulnerability, such as criminal groups, terrorists, bot-net operators, and disgruntled employees, or (2) a situation and method that may accidentally trigger a vulnerability such as an undocumented process, severe storm, and accidental or unintentional behavior.
- A ***vulnerability*** is a weakness that could be exploited by a threat source. Vulnerabilities can be physical (for example, unlocked door, insufficient fire suppression), natural (for example, facility located in a flood zone or in a hurricane belt), technical (for example, misconfigured systems, poorly written code), or human (for example, untrained or distracted employee).
- ***Impact*** is the magnitude of harm.
- The ***likelihood of occurrence*** is a weighted factor or probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).
- A ***control*** is a security measure designed to prevent, deter, detect, or respond to a threat source.
- ***Residual risk*** is the level of risk after security measures are applied. In its most simple form, residual risk can be defined as the likelihood of occurrence after controls are applied, multiplied by the expected loss. Residual risk is a reflection of the actual state. As such, the risk level can run the gamut from severe to nonexistent.

Let's consider the *threat* of obtaining unauthorized access to protected customer data. A *threat source* could be a cybercriminal. The *vulnerability* is that the information system that stores the data is Internet facing. We can safely assume that if no security measures were in place, the criminal would have unfettered access to the data (*inherent risk*). The resulting harm (*impact*) would be reputational damage, cost of responding to the breach, potential lost future revenue, and perhaps regulatory penalties. The security measures in place include data access controls, data encryption, ingress and egress filtering, an intrusion detection system, real-time activity monitoring, and log review. The *residual risk* calculation is based on the likelihood that the criminal (*threat source*) would be able to successfully penetrate the security measures, and if so what the resulting harm would be. In this example, because the stolen or accessed data are encrypted, one could assume that the residual risk would be low (unless, of course, they were also able to access the decryption key). However, depending on the type of business, there still might be an elevated reputation risk associated with a breach.

FYI: Business Risk Categories

In a business context, risk is further classified by category, including strategic, financial, operational, personnel, reputational, and regulatory/compliance risk:

- ***Strategic*** risk relates to adverse business decisions.
- ***Financial*** (or investment) risk relates to monetary loss.
- ***Reputational*** risk relates to negative public opinion.

- ***Operational*** risk relates to loss resulting from inadequate or failed processes or systems.
- ***Personnel*** risk relates to issues that affect morale, productivity, recruiting, and retention.
- ***Regulatory/compliance*** risk relates to violations of laws, rules, regulations, or policy.

Risk Assessment Methodologies

Components of a risk assessment methodology include a defined process, a risk model, an assessment approach, and standardized analysis. The benefit of consistently applying a risk assessment methodology is comparable and repeatable results. The three most well-known information security risk assessment methodologies are OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, developed at the CERT Coordination Center at Carnegie Mellon University), FAIR (Factor Analysis of Information Risk), and the NIST Risk Management Framework (RMF). The NIST Risk Management Framework includes both risk assessment and risk management guidance.

NIST Risk Assessment Methodology

Federal regulators and examiners often refer to NIST SP 800-30 and SP 800-39 in their commentary and guidance. The NIST Risk Assessment methodology, as defined in SP 800-30: Guide to Conducting Risk Assessments, is divided into four steps: Prepare for the assessment, conduct the assessment, communicate the results, and maintain the assessment. It is unrealistic that a single methodology would be able to meet the diverse needs of private and public sector organizations. The expectation set forth in NIST SP 800-39 and 800-30 is that each organization will adapt and customize the methodology based on size, complexity, industry sector, regulatory requirements, and threat vector.

In Practice

Information Security Risk Assessment Policy

Synopsis: To assign responsibility for and set parameters for conducting information security risk assessments.

Policy Statement:

- The company must adopt an information security risk assessment methodology to ensure consistent, repeatable, and comparable results.
- Information security risk assessments must have a clearly defined and limited scope. Assessments with a broad scope become difficult and unwieldy in both their execution and the documentation of the results.
- The CISO is charged with developing an information security risk assessment schedule based on the information system's criticality and information classification level.

- In addition to scheduled assessments, information security risk assessments must be conducted prior to the implementation of any significant change in technology, process, or third-party agreement.
- The CISO and the business process owner are jointly required to respond to risk assessment results and develop risk reduction strategies and recommendations.
- Risk assessment results and recommendations must be presented to executive management.

What Is Risk Management?

Risk management is the process of determining an acceptable level of risk (risk appetite and tolerance), calculating the current level of risk (risk assessment), accepting the level of risk (risk acceptance), or taking steps to reduce risk to the acceptable level (risk mitigation). We discussed the first two components in the previous sections.

Risk Acceptance

Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process. Generally, but not always, this means that the outcome of the risk assessment is within tolerance. There may be times when the risk level is not within tolerance but the organization will still choose to accept the risk because all other alternatives are unacceptable. Exceptions should always be brought to the attention of management and authorized by either the executive management or the Board of Directors.

Risk Mitigation

Risk mitigation implies one of four actions—reducing the risk by implementing one or more countermeasures (risk reduction), sharing the risk with another entity (risk sharing), transferring the risk to another entity (risk transference), modifying or ceasing the risk-causing activity (risk avoidance), or a combination thereof.

Risk mitigation is a process of reducing, sharing, transferring, or avoiding risk. ***Risk reduction*** is accomplished by implementing one or more offensive or defensive controls in order to lower the residual risk. An ***offensive control*** is designed to reduce or eliminate vulnerability, such as enhanced training or applying a security patch. A ***defensive control*** is designed to respond to a threat source (for example, a sensor that sends an alert if an intruder is detected). Prior to implementation, risk reduction recommendations should be evaluated in terms of their effectiveness, resource requirements, complexity impact on productivity and performance, potential unintended consequences, and cost. Depending on the situation, risk reduction decisions may be made at the business unit level, by management or by the Board of Directors.

Risk transfer or risk sharing is undertaken when organizations desire and have the means to shift risk liability and responsibility to other organizations. ***Risk transfer*** shifts the entire risk responsibility or liability from one organization to another organization. This is often accomplished by purchasing insurance. ***Risk sharing*** shifts a portion of risk responsibility or liability to other organizations. The caveat to this option is that regulations such as GLBA (financial institutions) and HIPAA/HITECH (healthcare organizations) prohibit covered entities from shifting compliance liability.

Risk avoidance may be the appropriate risk response when the identified risk exceeds the organizational risk appetite and tolerance, and a determination has been made not to make an exception. ***Risk avoidance*** involves taking specific actions to eliminate or significantly modify the process or activities that are the basis for the risk. It is unusual to see this strategy applied to critical systems and processes because both prior investment and opportunity costs need to be considered. However, this strategy may be very appropriate when evaluating new processes, products, services, activities, and relationships.

In Practice

Information Security Risk Response Policy

Synopsis: To define information security risk response requirements and authority.

Policy Statement:

- The initial results of all risk assessments must be provided to executive management and business process owner within seven days of completion.
- Low risks can be accepted by business process owners.
- Elevated risks and severe risks (or comparable rating) must be responded to within 30 days. Response is the joint responsibility of the business process owner and the CISO. Risk reduction recommendations can include risk acceptance, risk mitigation, risk transfer, risk avoidance, or a combination thereof. Recommendations must be documented and include an applicable level of detail.
- Severe and elevated risks can be accepted by executive management.
- The Board of Directors must be informed of accepted severe risk. At their discretion, they can choose to overrule acceptance.

FYI: Cyber Insurance

Two general categories of risks and potential liabilities are covered by cyber-insurance: first-party risks and third-party risks:

- ***First-party risks*** are potential costs for loss or damage to the policyholder's own data, or lost income or business.
- ***Third-party risks*** include the policyholder's potential liability to clients or to various governmental or regulatory entities.
- A company's optimal cyber-security policy would contain coverage for both first- and third-party claims. A 2013 Ponemon Institute Study commissioned by Experian Data Breach Resolution found that of 683 surveys completed by risk management professionals across multiple business sectors that have considered or adopted cyber-insurance, 86% of policies covered notification costs, 73% covered legal defense costs, 64% covered forensics and investigative costs, and 48% covered replacement of lost or damaged equipment. Not everything was always covered, though, as companies said only 30% of policies covered third-party liability, 30% covered communications costs to regulators, and 8% covered brand damages.

FYI: Small Business Note

Policy, governance, and risk management are important regardless of the size of the organization. The challenge for small organizations is who is going to accomplish these tasks. A small (or even a mid-size) business may not have a Board of Directors, C-level officers, or directors. Instead, as illustrated in Table 4.2, tasks are assigned to owners, managers, and outsourced service providers. What does not change regardless of size is the responsibilities of data owners, data custodians, and data users.

TABLE 4.2 Organizational Roles and Responsibilities

Role	Small Business Equivalent
Board of Directors	Owner(s).
Executive management	Owner(s) and/or management.
Chief Security Officer	A member of the management team whose responsibilities include information security. If internal expertise does not exist, external advisors should be engaged.
Chief Risk Officer	A member of the management team whose responsibilities include evaluating risk. If internal expertise does not exist, external advisors should be engaged.
Compliance Officer	A member of the management team whose responsibilities include ensuring compliance with applicable laws and regulations. If internal expertise does not exist, external advisors should be engaged.
Director of IT	IT manager. If internal expertise does not exist, external service providers should be engaged.
Internal audit	If this position is required, it is generally outsourced.

Summary

Information security is not an end unto itself. Information security is a business discipline that exists to support business objectives, add value, and maintain compliance with externally imposed requirements. This type of relationship is known as *strategic alignment*. Organizational commitment to information security practices should be codified in a written policy. The information security policy is an authoritative document that informs decision making and practices. As such, it should be authorized by the Board of Directors or equivalent body. Derivative documents for specific audiences should be published and distributed. This includes an Acceptable Use Policy and Agreement for users, a third-party version for vendors and service providers, and a synopsis for business partners and clients.

It is essential that information security policies remain relevant and accurate. At a minimum, policies should be reviewed and reauthorized annually. Change drivers are events that modify how a company operates and are a trigger for policy review. Compliance with policy requirements should be assessed and reported to executive management.

An *information security audit* is a systematic evidence-based evaluation of how well the organization conforms to established criteria. Audits are generally conducted by independent auditors, which implies that the auditor is not responsible for, benefited from, or in any way influenced by the audit target. A *capability maturity model (CMM) assessment* is an evaluation of process maturity for a given area. In contrast to an audit, the application of a CMM is generally an internal process. Audits and maturity models are good indicators of policy acceptance and integration.

Governance is the process of managing, directing, controlling, and influencing organizational decisions, actions, and behaviors. The Board of Directors is the authoritative policy making body. Executive management is tasked with providing support and resources. Endorsed by the Board of Directors and executive management, the CISO (or equivalent role) is vested with information security program management responsibility and accountability. The chain of command for the CISO should be devoid of conflict of interest. The CISO should have the authority to communicate directly with the Board of Directors.

Discussion, debate, and thoughtful deliberation result in good decision making. Supporting the CISO should be an Information Security Steering Committee, whose members represent a cross-section of the organization. The steering committee serves in an advisory capacity with particular focus on the alignment of business and security objectives. Distributed throughout the organization are a variety of roles that have information security–related responsibilities. Most notably, data owners are responsible for defining protection requirements, data custodians are responsible for managing the protection mechanisms, and data users are expected to act in accordance with the organization's requirements and to be stewards of the information in their care.

Three factors influence information security decision making and policy development: guiding principles, regulatory requirements, and risks related to achieving their business objectives. *Risk* is the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction. *Risk tolerance* is how much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit. *Risk management* is the process of determining an acceptable level of risk, identifying the level of risk for a given situation, and determining if the risk should be accepted or mitigated. A *risk assessment* is used to calculate the level of risk. A number of publically available risk assessment methodologies are available for organizations to use and customize. Risk acceptance indicates that the organization is willing to accept the level of risk associated with a given activity or process. Risk mitigation implies that one of four actions (or a combination of actions) will be undertaken: risk reduction, risk sharing, risk transference, or risk avoidance.

Risk management, governance, and information policy are the basis of an information program. Policies related to these domains include the following policies: Information Security Policy, Information Security Policy Authorization and Oversight, CISO, Information Security Steering Committee, Information Security Risk Management Oversight, Information Security Risk Assessment, and Information Security Risk Management.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. When an information security program is said to be "strategically aligned," this indicates that ___________________.

   A. It supports business objectives

   B. It adds value

   C. It maintains compliance with regulatory requirements

   D. All of the above

2. How often should information security policies be reviewed?

   A. Once a year

   B. Only when a change needs to be made

   C. At a minimum, once a year and whenever there is a change trigger

   D. Only as required by law

3. Information security policies should be authorized by ____________.

   A. the Board of Directors (or equivalent)

   B. business unit managers

   C. legal counsel

   D. stockholders

4. Which of the following statements best describes policies?

   A. Policies are the implementation of specifications.

   B. Policies are suggested actions or recommendations.

   C. Policies are instructions.

   D. Policies are the directives that codify organizational requirements.

5. Which of the following statements best represents the most compelling reason to have an employee version of the comprehensive information security policy?

   A. Sections of the comprehensive policy may not be applicable to all employees.

   B. The comprehensive policy may include unknown acronyms.

   C. The comprehensive document may contain confidential information.

   D. The more understandable and relevant a policy is, the more likely users will positively respond to it.

6. Which of the following is a common element of all federal information security regulations?

   A. Covered entities must have a written information security policy.

   B. Covered entities must use federally mandated technology.

   C. Covered entities must self-report compliance.

   D. Covered entities must notify law enforcement if there is a policy violation.

7. Organizations that choose to adopt the ISO 27002:2103 framework must ________________.

   A. use every policy, standard, and guideline recommended

   B. create policies for every security domain

   C. evaluate the applicability and customize as appropriate

   D. register with the ISO

8. Evidence-based techniques used by information security auditors include which of the following elements?

   A. Structured interviews, observation, financial analysis, and documentation sampling

   B. Structured interviews, observation, review of practices, and documentation sampling

   C. Structured interviews, customer service surveys, review of practices, and documentation sampling

   D. Casual conversations, observation, review of practices, and documentation sampling

9. Which of the following statements best describes independence in the context of auditing?

   A. The auditor is not an employee of the company.

   B. The auditor is certified to conduct audits.

   C. The auditor is not responsible for, benefited from, or in any way influenced by the audit target.

   D. Each auditor presents his or her own opinion.

10. Which of the following states is *not* included in a CMM?

    A. Average

    B. Optimized

    C. Ad hoc

    D. Managed

11. Which of the following activities is not considered a governance activity?

    A. Managing

    B. Influencing

    C. Evaluating

    D. Purchasing

12. To avoid conflict of interest, the CISO could report to which of the following individuals?

    A. The Chief Information Officer (CIO)

    B. The Chief Technology Officer (CTO)

    C. The Chief Financial Officer (CFO)

    D. The Chief Compliance Officer (CCO)

13. Which of the following statements best describes the role of the Information Security Steering Committee?

    A. The committee authorizes policy.

    B. The committee serves in an advisory capacity.

    C. The committee approves the InfoSec budget.

    D. None of the above.

14. Defining protection requirements is the responsibility of ____________.

    A. the ISO

    B. the data custodian

    C. data owners

    D. the Compliance Officer

15. Designating an individual or team to coordinate or manage information security is required by _________.

    A. GLBA
    B. MA CMR 17 301
    C. PCI DSS
    D. All of the above

16. Which of the following terms best describes the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and/or inaction?

    A. Threat
    B. Risk
    C. Vulnerability
    D. Impact

17. Inherent risk is the state before __________________.

    A. an assessment has been conducted
    B. security measures have been implemented
    C. the risk has been accepted
    D. None of the above

18. Which of the following terms best describes the natural, environmental, or human event or situation that has the potential for causing undesirable consequences or impact?

    A. Risk
    B. Threat source
    C. Threat
    D. Vulnerability

19. Which of the following terms best describes a disgruntled employee with intent to do harm?

    A. Risk
    B. Threat source
    C. Threat
    D. Vulnerability

20. Which if the following activities is *not* considered an element of risk management?

    A. The process of determining an acceptable level of risk

    B. Assessing the current level of risk for a given situation

    C. Accepting the risk

    D. Installing risk-mitigation safeguards

21. How much of the undesirable outcome the risk taker is willing to accept in exchange for the potential benefit is known as _________.

    A. risk acceptance

    B. risk tolerance

    C. risk mitigation

    D. risk avoidance

22. Which of the following statements best describes a vulnerability?

    A. A vulnerability is a weakness that could be exploited by a threat source.

    B. A vulnerability is a weakness that can never be fixed.

    C. A vulnerability is a weakness that can only be identified by testing.

    D. A vulnerability is a weakness that must be addressed regardless of the cost.

23. A control is a security measure that is designed to _______ a threat source.

    A. detect

    B. deter

    C. prevent

    D. All of the above

24. Which of the following is not a risk-mitigation action?

    A. Risk acceptance

    B. Risk sharing or transference

    C. Risk reduction

    D. Risk avoidance

25. Which of the following risks is best described as the expression of (the likelihood of occurrence after controls are applied) × (expected loss)?

    A. Inherent risk

    B. Expected risk

    C. Residual risk

    D. Accepted risk

26. Which of the following risk types best describes an example of insurance?

- **A.** Risk avoidance
- **B.** Risk transfer
- **C.** Risk acknowledgement
- **D.** Risk acceptance

27. Which of the following risk types relates to negative public opinion?

- **A.** Operational risk
- **B.** Financial risk
- **C.** Reputation risk
- **D.** Strategic risk

28. Compliance risk as it relates to federal and state regulations can never be ____________.

- **A.** avoided
- **B.** transferred
- **C.** accepted
- **D.** None of the above

29. Which of the following statements best describes organizations that are required to comply with multiple federal and state regulations?

- **A.** They must have different policies for each regulation.
- **B.** They must have multiple ISOs.
- **C.** They must ensure that their information security program includes all applicable requirements.
- **D.** They must choose the one regulation that takes precedence.

30. Which of the following terms best describes "duty of care" as applied to corporate directors and executive officers?

- **A.** It's a legal obligation.
- **B.** It's an outdated requirement.
- **C.** It's ignored by most organizations.
- **D.** It's a factor only when there is a loss greater than $1,000.

EXERCISES

EXERCISE 4.1: Understanding ISO 27002:2005

The introduction to ISO 27002:2005 includes this statement: "This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required."

1. Explain how this statement relates to the concept of strategic alignment.
2. The risk assessment domain was included in the ISO 27002:2005 edition and then removed in ISO 27002:2013. Why do you think they made this change?
3. What are the major topics of ISO 27005?

EXERCISE 4.2: Understanding Policy Development and Authorization

Three entrepreneurs got together and created a website design hosting company. They will be creating websites and social media sites for their customers, from simple "Hello World" pages to full-fledged e-commerce solutions. One entrepreneur is the technical guru, the second is the marketing genius, and the third is in charge of finances. They are equal partners. The entrepreneurs also have five web developers working for them as independent contractors on a per-project basis. Customers are requesting a copy of their security policies.

1. Explain the criteria they should use to develop their policies. Who should authorize the policies?
2. Should the policies apply to the independent contractors? Why or why not?
3. What type of documentation should they provide their customers?

EXERCISE 4.3: Understanding Information Security Officers

1. ISOs are in high demand. Using online job hunting sites (such as Monster.com, Dice.com, and TheLadders.com), research available positions in your geographic area.
2. Is there a common theme in the job descriptions?
3. What type of certifications, education, and experience are employers seeking?

EXERCISE 4.4: Understanding Risk Terms and Definitions

1. Define each of the following terms: inherent risk, threat, threat source, vulnerability, likelihood, impact, and residual risk.
2. Provide examples of security measures designed to (a) deter a threat source, (b) prevent a threat source from being successful, and (c) detect a threat source.
3. Explain risk avoidance and why that option is generally not chosen.

EXERCISE 4.5: Understanding Insurance

1. What is cyber-insurance and what does it generally cover?
2. Why would an organization purchase cyber-insurance?
3. What is the difference between first-party coverage and third-party coverage?

PROJECTS

PROJECT 4.1: Analyzing a Written Policy

1. Many organizations rely on institutional knowledge rather than written policy. Why do you think all major information security regulations require a written information security policy? Do you agree? Explain your opinion.
2. We are going to test the conventional wisdom that policy should be documented conducting an experiment.

   a. Write down or print out these three simple policy statements. Or, if you would prefer, create your own policy statements.

      The Board of Directors must authorize the Information Security Policy.

      An annual review of the Information Security Policy must be conducted.

      The CISO is responsible for managing the review process.

   b. Enlist four subjects for your experiment.

      Give two of the subjects the written policy. Ask them to read document. Have them keep the paper.

      Read the policy to the two other subjects. Do not give them a written copy.

   c. Within 24 hours, contact each subject and ask them to recall as much of the policy as possible. If they ask, let the first two subjects know that they can consult the document you gave them. Document your findings. Does the outcome support your answer to Question 1?

PROJECT 4.2: Analyzing Information Security Management

1. Does your school or workplace have a CISO or an equivalent position? Who does the CISO (or equivalent) report to? Does he or she have any direct reports? Is this person viewed as a security champion? Is he or she accessible to the user community?
2. It is important that CISOs stay current with security best practices, regulations, and peer experiences. Research and recommend (at least three) networking and educational resources.
3. If you were tasked with selecting an Information Security Steering Committee at your school or workplace to advise the CISO (or equivalent), who would you choose and why?

PROJECT 4.3: **Using Risk Assessment Methodologies**

The three most well-known information security risk assessment methodologies are OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation, developed at the CERT Coordination Center at Carnegie Mellon University), FAIR (Factor Analysis of Information Risk), and the NIST Risk Management Framework (RMF).

1. Research and write a description of each (including pros and cons).
2. Are they in the public domain, or is there a licensing cost?
3. Is training available?

Case Study

Determining the Likelihood and Impact of Occurrence

One of the most challenging aspects of a risk assessment is determining the likelihood of occurrence and impact. NIST SP 800-30 defines the likelihood of occurrence as follows: A weighted risk factor based on an analysis of the probability that a given threat source is capable of exploiting a given vulnerability (or set of vulnerabilities). For adversarial threats, an assessment of likelihood of occurrence is typically based on: (i) adversary *intent*; (ii) adversary *capability*; and (iii) adversary *targeting*. For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data, or other factors. Organizations typically employ a three-step process to determine the overall likelihood of threat events:

- Organizations assess the likelihood that threat events will be initiated (for adversarial threat events) or will occur (for non-adversarial threat events).
- Organizations assess the likelihood that the threat events, once initiated or occurring, will result in adverse impacts or harm to organizational operations and assets, individuals, other organizations, or the nation.
- Organizations assess the overall likelihood as a combination of likelihood of initiation/occurrence and likelihood of resulting in adverse impact.

Identify two threat sources—one adversarial and one non-adversarial—that could exploit a vulnerability at your school or workplace and would result in disruption of service. An adversarial event is the *intentional* exploitation of a vulnerability by criminal groups, terrorists, bot-net operators, or disgruntled employees. A non-adversarial event is the *accidental* exploit of a vulnerability, such as an undocumented process, a severe storm, or accidental or unintentional behavior.

1. For each (using your best judgment), answer the following questions:

   a) What is the threat?

   b) What is the threat source?

   c) Is the source adversarial or non-adversarial?

d) What vulnerability could be exploited?

e) How likely is the threat source to be successful and why?

f) If the threat source is successful, what is the extent of the damage caused?

2. Risk assessments are rarely conducted by one individual working alone. If you were hosting a workshop to answer the preceding questions, who would you invite and why?

References

Regulations Cited

"Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards," accessed on 08/2013, www.fdic.gov/regulations/laws/rules/2000-8660.html.

"201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth," official website of the Office of Consumer Affairs & Business Regulation (OCABR), accessed on 05/06/2013, www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

"Family Educational Rights and Privacy Act (FERPA)," official website of the US Department of Education, accessed on 05/2013, www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

"HIPAA Security Rule," official website of the Department of Health and Human Services, accessed on 05/2013, www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

Other References

Allen, Julia, "Governing for Enterprise Security: CMU/SEI-2005-TN-023 2005," Carnegie Mellon University, June 2005.

Bejtlich, Richard, "Risk, Threat, and Vulnerability 101," accessed on 10/2013, http://taosecurity.blogspot.com/2005/05/risk-threat-and-vulnerability-101-in.html.

"Capability Maturity Model," accessed on 10/2013, http://en.wikipedia.org/wiki/Capability_Maturity_Model.

DeMauro, John, "Filling the Information Security Officer Role within Community Banks," accessed on 10/2013, www.practicalsecuritysolutions.com/articles/.

"Duty of Care," Legal Information Institute, Cornell University Law School, accessed on 10/2013, www.law.cornell.edu/wex/duty_of_care.

Godes, Scott, Esq., and Kristi Singleton, Esq. “Top Ten Tips for Companies Buying Cyber Security Insurance Coverage,” accessed on 10/2013, www.acc.com/legalresources/publications/topten/tttfcbcsic.cfm.

“Information Security Governance: Guidance for Boards of Directors and Executive Management, Second Edition,” IT Governance Institute, 2006.

“In re Caremark International Inc. Derivative Litigation,” accessed on 10/2013, http://en.wikipedia.org/wiki/In_re_Caremark_International_Inc._Derivative_Litigation.

Matthews, Chris, “Cybersecurity Insurance Picks Up Steam,” *Wall Street Journal/Risk & Compliance Journal*, August 7, 2013, accessed on 10/2013, http://blogs.wsj.com/riskandcompliance/2013/08/07/cybersecurity-insurance-picks-up-steam-study-finds/.

“PCI DDS Requirements and Security Assessment Procedures, Version 2.0,” PCI Security Standards Council LLC, October 2010.

“Process & Performance Improvement,” Carnegie Mellon Software Engineering Institute, accessed on 10/2013, www.sei.cmu.edu/process/.

“Risk Management,” accessed on 10/2013, http://en.wikipedia.org/wiki/Risk_management#Potential_risk_treatments.

Scott, Todd, Alex Talarides, and Jim Kramer. “Do directors face potential liability for not preventing cyber attacks?” June 24, 2013, accessed on 10/2013, www.lexology.com/library.

Swenson, David, Ph.D., “Change Drivers,” accessed on 10/2013, http://faculty.css.edu/dswenson/web/Chandriv.htm.

“The Security Risk Management Guide,” Microsoft, 2006.

“What Is the Capability Maturity Model (CMM)?” accessed on 10/2013, www.selectbs.com/process-maturity/what-is-the-capability-maturity-model.

Chapter 5

Asset Management

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Assign information ownership responsibilities.
- Develop and use information classification guidelines.
- Understand information handling and labeling procedures.
- Identify and inventory information systems.
- Create and implement asset classification policies.

Is it possible to protect something if we do not know how much it is worth and how sensitive it is? Until we classify the information, how do we know the level of protection required? Unless we determine the value to the organization, how can we decide the amount of time, effort, or money that we should spend securing the asset? Who is responsible for making these decisions? How do we communicate the value of our information assets to our employees, business partners, and vendors?

Identification and classification of information assets and systems is essential to the proper selection of security controls to *protect against loss* of confidentiality, integrity, and availability (CIA):

- A *loss of confidentiality* is the unauthorized disclosure of information.
- A *loss of integrity* is the unauthorized or unintentional modification or destruction of information.
- A *loss of availability* is the accidental or intentional disruption of access to or use of information or an information system.

In this chapter, we will be looking at the various methods and rating methodologies that organizations use to define, inventory, and classify information and information systems. We will examine public and private sector classification systems that are used to communicate value and handling instructions. We will determine who is responsible for these activities. Lastly, we will put these best practices into policy.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 8 of ISO 27002:2013 focuses on asset management with the objective of developing classification schema, assigning classification levels, and developing handling standards to protect information.

Corresponding NIST guidance is provided in the following documents:

- SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories (two volumes)
- SP 800-88: Guidelines for Media Sanitization

Information Assets and Systems

What exactly is an information asset and why protect it? An ***information asset*** is a definable piece of information, stored in any manner, that is recognized as having value to the organization. Information assets include raw, mined, developed, and purchased data. If the information is damaged, compromised, or stolen, the consequences could include embarrassment, legal liability, financial ruin, and even loss of life.

Examples of organizational information include the following:

- Data stores or warehouses of information about customers, personnel, production, sales, marketing, or finances.
- Intellectual property (IP) such as drawings, schematics, patents, music scores, or other publications that have commercial value.
- Operational and support procedures.
- Research documentation or proprietary information based on experimentation or exploration.
- Strategic and operational plans, processes, and procedures that uniquely define the organization.

Information systems are the supporting players. ***Information systems*** provide a way and a place to process, store, transmit, and communicate the information. These systems are generally a combination of hardware and software assets and associated services. Information systems can be garden-variety off-the-shelf products or highly customized equipment and code. Support services may be technical services (voice communication and data communication) or environmental (heating, lighting, air conditioning, and power). The location of information systems may be "on premises," at a contracted data center, or in the cloud.

Who Is Responsible for Information Assets?

This brings us to the question of ownership. Every information asset must be assigned an owner. The success of an information security program is directly related to the defined relationship between the data owner and the information. In the best-case scenario, the data owner also functions as a security champion enthusiastically embracing the goals of CIA.

In Chapter 3, "Information Security Framework," we defined information ownership as being liable and responsible for protecting the information and the business results derived from using that information. For example, you have a medical file at your doctor's office that may contain your medical history, digital scans, lab results, and physician notes. The clinicians in the office use that information to provide you with medical care. Because the information is all about you, are you the owner? No. The medical staff uses the information to provide care, so are they the owner? No. The information owner is the one responsible for protecting the *confidentiality* of your medical record, ensuring the *integrity* of the information in your records, and making sure that it is *available* to the clinicians whenever you need care. In a small medical practice, the owner is generally a physician. In a clinic or hospital, the owner is a member of senior management. Although it may seem obvious that every information asset needs an owner, it is not always apparent who should be or who is willing to assume the responsibility of ownership.

The Role of the Data Owner

The ISO 27002:2013 standard recommends that we have a policy that specifically addresses the need to account for our information assets and to assign an owner to the asset. The goal of an Information Ownership policy is to ensure that appropriate protection is maintained. Owners should be identified for all major information assets and given the responsibility for the safeguarding of the information system. The owner is responsible for the security of the asset. Data owner responsibilities include the following:

- Defining the asset
- Assigning value to the asset
- Defining the level of protection required
- Deciding who should have access to the asset

- Delegating day-to-day security and operational tasks
- Ongoing governance

However, the owner is not the one who will be tasked with implementing security controls. That responsibility can be delegated to the information custodians such as system administrators.

The Role of the Information Security Officer

The information owner is accountable for the protection of the information asset. The information custodian is responsible for managing the day-to-day controls. The role of the Information Security Officer (ISO) is to provide direction and guidance as to the appropriate controls and to ensure that controls are applied consistently throughout the organization. Whereas information owners and custodians focus on specific information assets, the ISO is responsible for the security of the entire organization. As such, the office of the ISO is the central repository of security information. The ISO publishes the classification criteria, maintains the information systems inventories, and implements broad strategic and tactical security initiatives.

In Practice

Information Ownership Policy Statement

Synopsis: A data owner is responsible for the protection of assigned information and system. Inclusive in this responsibility are decisions about classification of information, protection of information and information systems, and access to information and information systems.

Policy Statement:

- All information assets and systems must have an assigned owner.
- The Office of Information Security will maintain an inventory of information ownership.
- Owners are required to classify information and information systems in accordance with the organizational classification guidelines.
- Owners are responsible for determining the required level of protection.
- Owners must authorize internal information and information system access rights and permissions. Access rights and permissions must be reviewed and approved annually.
- Owners must authorize third-party access to information or information systems. This includes information provided to a third party.
- Implementation and maintenance of controls is the responsibility of the Office of Information Security; however, accountability will remain with the owner of the asset.

Information Classification

The objective of an ***information classification system*** is to differentiate data types. The value of an information classification system is to enable organizations to safeguard CIA based on content. The natural outcome of the classification process is instructions on who can access the asset, how the asset is to be used, what security measures need to be in place, and ultimately the method in which the asset should be destroyed or disposed of. Classification systems have their genesis in two seminal security models designed in the 1970s for the U.S. military: Bell-Lapadula and Biba. Both models are based on the assumption that an information system may contain information that requires different levels of security and that users of various clearance levels would be accessing the information system. The objective of the Bell-Lapadula model is to ensure confidentiality by restricting read access to data above what a user has permission to read and to restrict write access to data at a level below in order to minimize potential exposure. This is generally expressed as “no read up, no write down.” The objective of the Biba model is to ensure data integrity. The Biba model restricts users from reading data at a lower level and writing information to a higher level. The theory is that data at a lower level may be incomplete and/or inaccurate and if read could unduly influence what is written at a higher level. This is generally expressed as “no read down, no write up.” The implementation of Bell-Lapadula, Biba, and subsequent models required that a structured data classification system be developed.

Classification systems are now used in the private sector, the government, and the military. A financial institution will allow a teller to view general account information and cash checks of reasonable amounts. That same teller is not allowed to view information about internal bank assets and most definitely cannot access systems that would allow her to transfer millions of dollars. A hospital will allow a lab technician to access patient demographics and physician instructions but will not allow him to read or edit the complete patient record. The military, based on national security concerns, makes decisions to whom and how to make information accessible. They certainly do not want battle plans shared with the enemy. In fact, the military is a vivid example of an organization that relies extensively on a well-defined classification system. They classify not only information systems but people as well. Military and supporting civilian personnel are assigned clearance levels. The clearance level of the individual must match the classification of the data in order to be granted access. In this section, we are going to examine different approaches to information classification.

In Practice

Information Classification Lifecycle Process

An information classification lifecycle begins with the assignment of classification and ends with declassification. The information owner is responsible for managing this process, which is as follows:

- Document the information asset and the supporting information systems.
- Assign a classification level.
- Apply the appropriate labeling.

- Document “special” handling procedures (if different from organizational standards).
- Conduct periodic classification reviews.
- Declassify information when (and if) appropriate.

FYI: Freedom of Information Act

Enacted on July 4, 1966, and taking effect one year later, the Freedom of Information Act (FOIA) provides a powerful tool to advocates for access to information. Under the FOIA, anyone may request and receive any records from federal agencies unless the documents can be officially declared exempt based on specific categories, such as Top Secret, Secret, and Classified. In 2012, there were 651,254 FOIA requests! To learn more about FOIA, explore for FOIA data, or make a FOIA request, visit FOIA.gov. The site includes highlights of newly released information ranging from a declassified secret spy satellite recovery mission to “ale to the chief”—the White House recipes for brewing beer!

How Does the Federal Government Classify Data?

Let’s start with looking at how federal agencies categorize information and systems and then compare how the private sector classifies information. The United States government has enormous amounts of data and has a vested responsibility in protecting the CIA of the information and information systems. To this end, federal guidelines require that federal agencies categorize information and information systems. Federal Information Processing Standard 199 (FIPS-199) requires that information owners classify information and information systems as ***low***, ***moderate***, or ***high security*** based on CIA criteria. The generalized format for expressing the security category (SC) of an information type is as follows: The SC of information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}, where the acceptable values for potential impact are low, moderate, high, or not applicable:

- ***Low potential impact*** means the loss of CIA could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals.
- ***Moderate potential impact*** means the loss of CIA could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals.
- ***High potential impact*** means the loss of CIA could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals.

Confidentiality Factors

Information is evaluated for confidentiality with respect to the impact of unauthorized disclosure as well as the use of the information. Federal guidelines suggest that agencies consider the following:

- How can a malicious adversary use the unauthorized disclosure of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- How can a malicious adversary use the unauthorized disclosure of information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/serious/severe harm to agency operations, agency assets, or individuals?
- Would unauthorized disclosure/dissemination of elements of the information type violate laws, executive orders (EOs), or agency regulations?

Integrity Factors

Information is evaluated for integrity with respect to the impact associated with unauthorized modification or destruction. Federal guidelines suggest that agencies consider the following:

- How does unauthorized or unintentional modification of information harm agency operations, agency assets, or individuals?
- What is the impact of actions taken, decisions made based on modified information, or if the modified information is disseminated to other organizations or the public?
- How does unauthorized or unintentional destruction of information harm agency operations, agency assets, or individuals?
- Does modification/destruction of elements of the information type violate laws, EOs, or agency regulations?

Availability Factors

Information is evaluated for availability with respect to the impact of disruption of access to or use of the information. Federal guidelines suggest that agencies consider the following:

- How does the disruption of access to or use of information do harm to agency operations, agency assets, or individuals?
- What is the impact of destruction and/or permanent loss of information?
- Does disruption of access to or use of elements of the information type violate laws, EOs, or agency regulations?

FYI: Examples of FIPS-199 Classification

Example 1: An organization managing *public information* on its web server determines that there is no potential impact from a loss of confidentiality (that is, confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting SC of this information type is expressed as follows:

SC public information = {(confidentiality, n/a), (integrity, moderate), (availability, moderate)}.

Example 2: A law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting SC for this type of information is expressed as follows:

SC investigative information = {(confidentiality, high), (integrity, moderate), (availability, moderate)}.

Example 3: A power plant contains an SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is moderate impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting SCs of these information types are expressed as follows:

SC sensor data = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}, and

SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

The resulting SC of the information system is expressed as

SC SCADA system = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)},

thus representing the high-water mark or maximum potential impact values for each security objective from the information type's resident on the SCADA system.

Why Is National Security Information Classified Differently?

The Unites States government and military process, store, and transmit information directly related to national security. It is important that everyone who interacts with these data recognize the significance. The first EO specifically defining and classifying government information was issued by President Harry S. Truman in 1952. Subsequent EOs were issued by Presidents Eisenhower, Nixon, Carter, Reagan, Clinton, and Bush. In December 2009, President Barack Obama issued Executive Order 13526 (Classified National Security Information), which revoked and replaced previous EOs:

“This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nations progress depends on the free flow of information. Nevertheless, throughout our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation’s security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities.” (President Barack Obama, December 29, 2009)

The following three special classifications defined in Executive Order 13526 denote special access and handling requirements. Information extraneous to the classification system is considered unclassified. Sensitive But Unclassified (SBU) is a Department of Defense–specific classification category. Authorization to assign classification level is restricted to specific U.S. Government officials:

- **Top Secret (TS)**—Any information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptology and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

- **Secret (S)**—Any information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

- **Confidential (C)**—Any information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security. Examples of damage include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; and revelation of performance characteristics, test data, design, and production data on munitions of war.

- **Unclassified (U)**—Any information that can generally be distributed to the public without any threat to national interest. Note: This category is not specifically defined in EO 13526.

- **Sensitive But Unclassified (SBU)**—This classification is a Department of Defense subcategory and is applied to "any information of which the loss, misuse or unauthorized access to, or modification of might *adversely affect* U.S. National Interests, the conduct of the Department of Defense (DoD) programs or the privacy of DoD personnel." Labeling in this category includes "For Official Use Only," "Not for Public Release," and "For Internal Use Only."

FYI: Edward Snowden: Hero or Traitor?

On June 14, 2013, the U.S. Government brought criminal charges against Edward Snowden, a former National Security Agency (NSA) contract employee who leaked to the media details of two top-secret surveillance programs known collectively as PRISM. One program collected billions of U.S. phone records. The second gathered audio, video, email, photographic, and Internet search usage of foreign nationals overseas, and probably some Americans in the process, who use major providers such as Microsoft, Google, Apple, and Yahoo!. Snowden had top-secret clearance and had been granted access to information about both programs.

Snowden fled the country carrying four laptop computers, after leaving his job at the NSA's eavesdropping station in Hawaii. He gave hundreds of highly classified documents to the British newspaper *The Guardian*, which wrote a series of articles about the U.S. Government programs. Snowden said he did so—even though he knew he was violating the law—because he could not live, in good conscience, with Americans secretly being denied their freedom and their right of privacy.

A one-page criminal complaint says Snowden engaged in unauthorized communication of national defense information and willful communication of classified communications intelligence information. Both are charges under the Espionage Act. Snowden also is charged with theft of government property. All three crimes carry a maximum ten-year prison penalty. Some consider him a traitor for violating the trust of his country; others see him as a hero who acted out of conscience to protect "basic liberties for people around the world."

Who Decides How National Security Data Is Classified?

National security data is classified in one of two ways:

- ***Original classification*** is the initial determination that information requires protection. Only specific U.S. Government officials who have been trained in classification requirements have the authority to make the classification decisions. Original classification authorities issue security classification guides that others use in making derivative classification decisions. Most government employees and contractors make derivative classification decisions.

- ***Derivative classification*** is the act of classifying a specific item of information or material based on an original classification decision already made by an authorized original classification authority. The source of authority for derivative classification ordinarily consists of a previously classified document or a classification guide issued by an original classification authority.

How Does the Private Sector Classify Data?

There are no legally mandated private sector data classifications so organizations are free to develop a classification system appropriate to their organization. Commonly used classifications include Legally Protected, Confidential, Internal Use, and Public. Information owners are responsible for classifying data and systems. Based on the classification, information custodians can apply the appropriate controls and, importantly, users know how to interact with the data.

- **Protected—**Data that is protected by law, regulation, memorandum of agreement, contractual obligation, or management discretion. Examples include non-public personal information (NPPI), such as social security number, driver's license or state-issued identification number, bank account or financial account numbers, payment card information (PCI), which is credit or debit cardholder information, and personal health information (PHI).
- **Confidential**—Data that is essential to the mission of an organization. Loss, corruption, or unauthorized disclosure would cause *significant* financial or legal damage to the organization and its reputation. Examples include business strategies, financial positions, employee records, upcoming sales or advertising campaigns, laboratory research, and product schematics.
- **Internal Use**—Data that is necessary for conducting ordinary company business. Loss, corruption, or unauthorized disclosure *may* impair the business or result in business, financial, or legal loss. Examples include policy documents, procedure manuals, non-sensitive client or vendor information, employee lists, or organizational announcements.
- **Public**—Information that is specifically intended for the public at large. Public information requires discretionary treatment and should be cleared for release prior to public distribution. This category includes annual reports, product documentation, list of upcoming trade shows, and published white papers.

If the appropriate classification is not inherently obvious, a conservative approach is generally used and the data is classified in the more restrictive category.

FYI: What Is NPPI and Why Protect It?

Non-public personal information (NPPI) is data or information considered to be personal in nature, subject to public availability, and if disclosed is an invasion of privacy. Compromise of NPPI is often a precursor to identity theft. NPPI is protected from disclosure and/or requires notification of disclosure by a variety of federal and state laws and regulations.

NPPI is defined as an individual's first name (or first initial) and last name linked with any one or more of the following data elements:

- Social security number
- Driver's license number
- Date of birth

- Credit or debit card numbers
- State identification card number
- Financial account number, in combination with any required security code, access code, or password that would permit access to the account

In Practice

Information Classification Policy

Synopsis: An information classification system will be used to categorize information and information systems. The classification will be used to design and communicate baseline security controls.

Policy Statement:

- The company will use a four-tiered data classification schema consisting of protected, confidential, restricted, and public.
- The company will publish definitions for each classification.
- The criteria for each level will be maintained by and available from the Office of Information Security.
- All information will be associated with one of the four data classifications. It is the responsibility of information owners to classify data.
- Information systems containing information from multiple classification levels will be secured in accordance with the requirements of the highest classification level.
- Data classification will remain in force regardless of the location or state of the data at any given time. This includes backup and archive mediums and locations.
- The classification system will allow that classifications of information assets may change over time.
- Each classification will have handling and protection rules. The Office of Information Security is responsible for the development and enforcement of the handling and protection rules.

Can Information Be Reclassified or Even Declassified?

Over a period of time, the need to protect information may change. An example of this can be found in the auto industry. Prior to a new car introduction, the design information is considered confidential. Disclosure would have serious ramifications to the automaker. After introduction, the same information is considered public and is published in the automotive manual. The process of downgrading sensitivity levels is known as ***declassification***.

Conversely, organizations may choose to strengthen the classification level if they believe that doing so is for the benefit of the organization or required by evolving regulations. For example, in 2013, HIPAA regulations were extended to cover data maintained by business associates. In this case, business associates need to revisit the classification of data they access, store, process, or transmit. The process of upgrading a classification is known as ***reclassification***. If the information owner knows ahead of time when the information should be reclassified, then that date should be noted on the original classification label (for example, "Confidential until [date]"). At the time an organization is establishing the criteria for classification levels, it should also include a mechanism for reclassifying and declassifying information. This responsibility may be assigned to the information owner or subject to an internal review process.

Labeling and Handling Standards

Information owners classify information in order to identify the level of protection necessary. As we defined in Chapter 2, "Policy Elements and Style," standards serve as specifications for the implementation of policy and dictate mandatory requirements. Handling standards dictate by classification level how information must be stored, transmitted, communicated, accessed, retained, and destroyed. ***Labeling*** is the vehicle for communicating the assigned classification to information custodians and users.

Why Label?

Labels make it easy to identify the data classification. Labels can take many forms: electronic, print, audio, and visual. Information may need to be labeled in many ways, depending on the audience. The labels you are probably most familiar with are safety labels. You recognize poison from the skull-and-crossbones symbol. You instinctively know to stop when you see a red stop sign. You know to pull over when you hear a police siren. In order to protect information, classification level labels need to be as clear and universally understood as a skull-and-crossbones symbol or a stop sign. Labels transcend institutional knowledge and provide stability in environments that experience personnel turnover.

In electronic form, the classification should be a part of the document name (for example, "Customer Transaction History–PROTECTED"). On written or printed documents, the classification label should be clearly marked on the outside of the document as well as in either the document header or footer. Media, such as backup tapes, should be clearly labeled with words and (where appropriate) symbols.

Why Handling Standards?

Information needs to be handled in accordance with its classification. ***Handling standards*** inform custodians and users how to treat the information they use and the systems they interact with. Handling standards generally include storage, transmission, communication, access, retention, destruction, and disposal, and may extend to incident management and breach notification.

As illustrated in Table 5.1, it is important that handling standards be succinctly documented in usable format. The handling standards should be introduced during the orientation period and reintroduced as part of an Acceptable Use Policy and Agreement.

TABLE 5.1 Sample Handling Standards Matrix

Data-Handling Standard	"Protected"	"Confidential"	"Internal"
Data Storage (Servers)	Allowed as required for business purposes.	Allowed as required for business purposes.	Allowed as required for business purposes.
Data Storage (Workstations–Internal)	Not allowed.	Not allowed.	Allowed as required for business purposes.
Data Storage (Mobile Devices and Media)	Allowed as required for business purposes. Encryption required.	Allowed as required for business purposes. Encryption required.	Allowed as required for business purposes. Encryption highly recommended.
Data Storage (Workstations–Home)	Not allowed.	Not allowed.	Allowed as required for business purposes.
Data Storage (Removable Media for Backup Purposes)	Storage allowed as required for business purposes. Encryption required.	Allowed as required for business purposes. Encryption required.	Allowed as required for business purposes.
Internal Email	Should be avoided if possible.	Should be avoided if possible.	Allowed.
Instant Message or Chat	Not allowed.	Not allowed.	Allowed, but strongly discouraged.
External Email	Text allowed as required for business purposes. Encryption required. No attachments. Footer must indicate that the content is legally protected.	Text allowed as required for business purposes. Encryption required. No attachments.	Allowed. Encryption optional but strongly recommended.
External File Transfer	Must be pre-authorized by a SVP. Encryption required.	Must be pre-authorized by a SVP. Encryption required.	Allowed. Encryption optional but strongly recommended.
Remote Access	Multifactor authentication required.	Multifactor authentication required.	Multifactor authentication required.

Data-Handling Standard	"Protected"	"Confidential"	"Internal"
Data Retention	Refer to Legal Record Retention and Destruction Guidelines.	Refer to Company Record Retention and Destruction Guidelines.	Refer to Departmental Record Retention and Destruction Guidelines.
Electronic Data Disposal/ Destruction	Must be irrevocably destroyed. Destruction certification required.	Must be irrevocably destroyed.	Recommend irrevocable destruction.
Paper Document Disposal	Must be cross-shredded. Destruction certification required.	Must be cross-shredded.	Recommend cross-shred.
Paper Document Storage	Maintained in a secure storage area or locked cabinet.	Maintained in a secure storage area or locked cabinet.	No special requirements.
External Mail Carriers	Use commercial carrier or courier service. Envelope/box should be sealed in such a way that tampering would be obvious. Packages must be signed for.	Use commercial carrier or courier service. Envelope/box should be sealed in such a way that tampering would be obvious. Packages must be signed for.	No special requirements.
Outgoing Fax	Cover page should indicate the faxed information is legally protected.	Cover page should indicate the faxed information is confidential.	Cover page should indicate the faxed information is internal use.
Incoming Fax	Incoming faxes should be directed to the closest fax machine, and removed from the machine immediately.	Incoming faxes should be directed to closest fax machine, and removed from the machine immediately.	No special requirements.
Suspected Breach, Unauthorized Disclosure, or Compliance Violation Should Be Reported To:	Reported immediately to the ISO or Compliance Officer.	Reported immediately to the ISO or Supervisor.	Reported immediately to Supervisor.
Data Handling Questions Should Be Directed To:	ISO or Compliance Officer.	ISO or Supervisor.	Reported immediately to Supervisor.

In Practice

Information Classification Handling and Labeling Requirements Policy

Synopsis: The classification and handling requirements of information assets should be clearly identified.

Policy Statement:

- Each classification will have labeling standards.
- Data and information systems will be labeled in accordance with its classification.
- Each classification of data will have documented handling standards for the following categories: storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification.
- The Office of Information Security is responsible for the development and implementation of the labeling and handling standards.
- All employees, contractors, and affiliates will be provided or have access to written documentation that clearly describes the labeling and handling standards.
- All employees, contractors, and affiliates will be provided with a resource to whom questions can be directed.
- All employees, contractors, and affiliates will be provided with a resource to whom violations can be reported.

Information Systems Inventory

As amazing as it may seem, many organizations do not have an up-to-date inventory of information systems. This happens for any number of reasons. The most prevalent is a lack of centralized management and control. Departments within organizations are given the autonomy to make individual decisions, bring in systems, and create information independent of the rest of the organization. Corporate cultures that encourage entrepreneurial behavior are particularly vulnerable to this lack of structure. Another reason is the growth of corporations through acquisitions and mergers. Sometimes companies change so rapidly it becomes nearly impossible to manage information effectively. Generally, the plan is to consolidate or merge information and systems, but in reality, they often end up cohabitating.

What Should Be Inventoried?

Putting together a comprehensive physical inventory of information systems is a major task. The critical decision is choosing what attributes and characteristics of the information asset you want to record. The more specific and detailed the inventory, the more useful the inventory will be. Bear in mind that over time your inventory may have multiple purposes, including being used for criticality and risk analysis, business impact, and disaster recovery planning insurance coverage, and business valuation.

Hardware Assets

Hardware assets are visible and tangible pieces of equipment and media, such as:

- **Computer equipment**—Mainframe computers, servers, desktops, laptops, tablets, and smartphones
- **Printers**—Printers, copiers, scanners, fax machines, and multifunction devices
- **Communication and networking equipment**—IDS/IPSs, firewalls, modems, routers, access points, cabling, DSU/CSUs, and transmission lines
- **Storage media**—Magnetic tapes, disks, CDs, DVDs, and USBs
- **Infrastructure equipment**—Power supplies, air conditioners, and access control devices

Software Assets

Software assets are programs or code that provide the interface between the hardware, the users, and the data. Software assets generally fall into three categories:

- **Operation system software**—Operating systems are responsible for providing the interface between the hardware, the user, and the application. Examples include Microsoft Windows, Apple iOS, Linux, Unix, and FreeBSD.
- **Productivity software**—The objective of productivity software is to provide basic business functionality and tools. Examples include the mobile apps, the Microsoft Office Suite (Word, Excel, Publisher, and PowerPoint), Adobe Reader, Intuit Quick Books, and TurboTax.
- **Application software**—Application software is designed to implement the business rules of the organization and is often custom developed. Examples include programs that run complex machinery, process bank transactions, or manage lab equipment.

Asset Inventory Characteristics and Attributes

Each asset should have a ***unique identifier***. The most significant identifier is the device or program name. Although you may assume that the name is obvious, you'll often find that different users, departments, and audiences refer to the same information, system, or device differently. Best practices dictate that the organization chooses a naming convention for its assets and apply the standard consistently. The naming convention may include the location, vendor, instance, and date of service. For example, a Microsoft Exchange server located in New York City and connected to the Internet may be named MS_EX_NYC_1. A SQL database containing inventory records of women's shoes might be named SQL_SHOES_W. The name should also be clearly labeled on the device. The key is to be consistent, so that the names themselves become pieces of information. This is, however, a double-edged sword. We risk exposing asset information to the public if our devices are accessible or advertise them in any way. We need to protect this information consistent with all other valuable information assets.

An ***asset description*** should indicate what the asset is used for. For example, devices may be identified as computers, connectivity, or infrastructure. Categories can (and should) be subdivided. Computers can be broken down into domain controllers, application servers, database servers, web servers, proxy servers' workstations, laptops, tablets, smartphones, and smart devices. Connectivity equipment might include IDS/IPSs, firewalls, routers, satellites, and switches. Infrastructure might include HVAC, utility, and physical security equipment.

For hardware devices, the manufacturer name, model number, part number, serial number, and host name or alias should be recorded. The physical and logical addresses should also be documented. The physical address refers to the geographic location of the device itself or the device that houses the information. This should be as specific as possible. For example, APPS1_NYC is located at the East 21st Street office's second floor data center. The logical address is where the asset can be found on the organization's network. The logical address should reference the host name, the Internet Protocol (IP) address, and, if applicable, the Media Access Control (MAC) address. Host names are "friendly names" given to systems. The host name may be the actual name of the system or an alias used for easy reference. The IP address is the unique network address location assigned to this system. Lastly, the MAC address is a unique identifier assigned to network connectivity devices by the manufacturer of the device.

FYI: Logical Addresses

Every device connected to a network or the Internet must be uniquely identified. The MAC address, the IP address, and the domain name are all used to identify a device. These addresses are known as "logical" rather than "physical" because they have little or no relationship to the geographic location of the device.

- **MAC Address**—A Media Access Control (MAC) address is a hardware identification number that uniquely identifies a device. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card. MAC addresses are made up of six two-digit hexadecimal numbers, separated by colon. Example: 9c-d3-6d-b9-ff-5e.
- **IPv4 Address**—A numeric label that uniquely identifies a device on the Internet and/or on an internal network. The label consists of four groups of numbers between 0 and 255, separated by periods (dots). Example: 195.112.56.75.
- **IPv6 Address—**Similar in function to IPv4, IPv6 is a 128-bit identifier. An IPv6 address is represented as eight groups of four hexadecimal digits. Example: FE80:0000:0000:0000:0202:B3FF:FE1E:8329.
- **IP Domain Name**—Domain names serve as humanly memorable names for Internet connected devices (for example, www.yourschool.edu). The "yourschool.edu" section of the name is assigned by an Internet registrar and uniquely describes a set of devices. The "www" is an alias for a specific device. When you access a website, the full domain name is actually translated to an IP address, which defines the server where the website located. This translation is performed dynamically by a service called a domain name system (DNS).

Software should be recorded by publisher or developer, version number, revision, the department or business that purchased or paid for the asset number, and, if applicable, patch level. Software vendors often assign a serial number or "software key," which should be included in the record.

Last but not least, the controlling entity should be recorded. The controlling entity is the department or business that purchased or paid for the asset and/or is responsible for the ongoing maintenance and upkeep expense. The controlling entity's capital expenditures and expenses are reflected in its budgets, balance sheets, and profit and loss statements.

Removing, Disposing Of, or Destroying Company Property

Company assets should be accounted for at all times. If company property needs to move from its assigned location or be destroyed, there should be an asset management procedure. Documentation should be maintained so that at any time an audit will account for the location and possession of every piece of equipment or information. Asset disposal and destruction is discussed in Chapter 7, "Physical and Environmental Security."

In Practice

Inventory of Information System Assets Policy

Synopsis: All information systems should be inventoried and tracked.

Policy Statement:

- All information system assets will be identified and documented with their classification, owner, location, and other details according to standards published by the Office of Information Security.
- Company assets must be accounted for at all times.
- The Office of Information Security will maintain the inventory documentation.
- Copies of all inventory documentation will be included in the Business Continuity Plan.

FYI: Small Business Note

Is it necessary for small businesses to classify data? Emphatically, yes! It is very likely that a small business stores, processes, or transmits legally protected financial or medical data and/or is contractually obligated to protect debit and credit card information. At the very least, the company has information that for reasons related to either privacy or competition should not become public knowledge. Table 5.2 shows a combination three-tier data classification description and data-handling instructions for small businesses.

TABLE 5.2 Small Business Data Classification and Handling Instructions

Data Classification and Data Handling Instructions			
I. Data Classification Definitions			
Protected	Data that is protected by law, regulation, contractual obligation, or management discretion.		
Confidential	Data that should not be publicly disclosed.		
Public	Data that is specifically intended for the public at-large.		
II. Data Handling Instructions			
	Protected	**Confidential**	**Public**
Data Storage Servers	Allowed as required for business purposes.	Allowed as required for business purposes.	Allowed as required for business purposes.
Data Storage Workstations	Not allowed.	Not allowed.	Allowed as required for business purposes.
Data Storage Mobile Devices	Allowed as required for business purposes. Encryption required.	Allowed as required for business purposes. Encryption required.	Allowed as required for business purposes.
Data Storage Home Workstations	Not allowed.	Not allowed.	Allowed as required for business purposes.
Internal Email	Should be avoided if possible.	Allowed.	Allowed.
External Email	Must be sent using secure email.	Allowed.	Allowed.
External File Transfer	Must be sent using a secure file transfer program.	Must be sent using a secure file transfer program.	Allowed.
Remote Access	Requires multifactor authentication.	Requires multifactor authentication.	N/A
Disposal/ Destruction	Must be irrevocably destroyed.	Must be irrevocably destroyed.	N/A
Paper Documents	Maintained in a secure storage area or in a locked cabinet.	Maintained in a secure storage area or in a locked cabinet.	N/A
Questions and Concerns	Please direct all questions or concerns to your direct supervisor.		

Summary

You may have heard the phrase “security through obscurity.” This phase implies that there is a proportional relationship between keeping an asset hidden and its safety. The problem with this concept is that it is not practical, or even desirable, to keep our information and systems locked up. Information assets have value to the organization and are often used in day-to-day operations to accomplish its mission. The inverse to “security through obscurity” is “security through classification and labeling.” The best way to protect an information asset or system is to identify the confidentiality, integrity, and availability (CIA) requirements and then apply the appropriate safeguards and handling standards. The process of identification and differentiation is known as *classification*. Information owners are responsible for properly identifying and classifying the information for which they are responsible. Information custodians are tasked with implementing security controls.

FISMA requires that federal agency information owners classify their information and information systems as low, moderate, or high security based on criteria outlined in the FIPS-199. Information is evaluated for confidentiality with respect to the impact of unauthorized disclosure as well as the use of the information, integrity with respect to the impact associated with unauthorized modification or destruction, and availability with respect to the impact of disruption of access to or use of the information. Five special classifications are reserved for national security–related information that denotes special access and handling requirements: Top Secret, Secret, Confidential, Unclassified, and Sensitive But Unclassified (SBU). The process of downgrading a classification is known as *declassification.* The process of upgrading a classification is known as *reclassification*.

There are no comparable classification requirements for the private section. However, multiple state and federal statutes require all organizations to protect specific categories of information. The broadest category is non-public personal information (NPPI). NPPI is information considered to be personal in nature, subject to public availability, and if disclosed is an invasion of privacy. It is common for private sector organizations to adopt a three- or four-tier classification system that takes into account legal, privacy, and business confidentiality requirements. Labeling is the vehicle for communicating the assigned classification to information custodians and users. Handling standards inform custodians and users how to treat the information they use and the systems they interact with.

Information systems provide a way and a place to process, store, and transmit information assets. It is important to maintain an up-to-date inventory of hardware and software assets. Hardware assets are visible and tangible pieces of equipment and media. Software assets are programs or code that provides the interface between the hardware, the users, and the data. Descriptors may include what the asset is used for, its location, the unique hardware identification number known as a MAC address, the unique network identifier known as an IP address, host name, and domain name.

Organizational Asset Management policies include Information Ownership, Information Classification, Handling and Labeling Requirements, and Information Systems Inventory.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following terms best describes a definable piece of information, stored in any manner, that is recognized as having value to the organization?

   A. NPPI
   B. Information asset
   C. Information system
   D. Classified data

2. Information systems __________, __________, and __________ information.

   A. create, modify, and delete
   B. classify, reclassify, and declassify
   C. store, process, and transmit
   D. use, label, and handle

3. Information owners are responsible for which of the following tasks?

   A. Classifying information
   B. Maintaining information
   C. Using information
   D. Registering information

4. Which of the following roles is responsible for implementing and maintaining security controls?

   A. Information owner
   B. Information vendor
   C. Information user
   D. Information custodian

5. FIPS-199 requires that federal government information and information systems be classified as ____________.

   A. Low security
   B. Moderate security
   C. High security
   D. None of the above

6. Information classification systems are used in which of the following organizations?

   A. Government

   B. Military

   C. Financial institutions

   D. All of the above

7. FIPS requires that information be evaluated for _____________requirements with respect to the impact of unauthorized disclosure as well as the use of the information.

   A. integrity

   B. availability

   C. confidentiality

   D. secrecy

8. Which of the following National Security classifications requires the most protection?

   A. Secret

   B. Top Secret

   C. Confidential

   D. Unclassified

9. Which of the following National Security classifications requires the least protection?

   A. Secret

   B. Unclassified

   C. Confidential

   D. Sensitive But Unclassified (SBU)

10. The Freedom of Information Act (FOIA) allows anyone access to which of the following?

    A. Access to all government information just by asking

    B. Access to all classified documents

    C. Access to classified documents on a “need to know” basis

    D. Access to any records from federal agencies unless the documents can be officially declared exempt

11. Which of the following terms best describes the CIA attribute associated with the modification of information?

    A. Classified

    B. Integrity

    C. Availability

    D. Intelligence

12. Is it mandatory for all private businesses to classify information?

    A. Yes.

    B. Yes, but only if they want to pay less taxes.

    C. Yes, but only if they do business with the government.

    D. No.

13. Which of the following is not a criterion for classifying information?

    A. The information is not intended for the public domain.

    B. The information has no value to the organization.

    C. The information needs to be protected from those outside of the organization.

    D. The information is subject to government regulations.

14. Data that is considered to be personal in nature and, if disclosed, is an invasion of privacy and a compromise of security is known as which of the following?

    A. Non-personal public information

    B. Non-private personal information

    C. Non-public personal information

    D. None of the above

15. Most organizations restrict access to protected, confidential, and internal-use data to which of the following roles within the organization?

    A. Executives

    B. Information owners

    C. Users who have a “need to know”

    D. Vendors

16. Labeling is the vehicle for communicating classification levels to which of the following roles within the organization?

    A. Employees

    B. Information custodians

    C. Contractors

    D. All of the above

17. Which of the following terms best describes rules for how to store, retain, and destroy data based on classification?

    A. Handling standards
    B. Classification procedures
    C. Use policies
    D. Material guidelines

18. Which of the following terms best describes the process of removing restricted classification levels?

    A. Declassification
    B. Classification
    C. Reclassification
    D. Negative classification

19. Which of the following terms best describes the process of upgrading or changing classification levels?

    A. Declassification
    B. Classification
    C. Reclassification
    D. Negative classification

20. The impact of destruction and/or permanent loss of information is used to determine which of the following safeguards?

    A. Authorization
    B. Availability
    C. Authentication
    D. Accounting

21. Which of the following terms best describes an example of a hardware asset?

    A. Server
    B. Database
    C. Hammer
    D. Radio waves

22. Which of the following statements best describes a MAC address?

    A. A MAC address is a unique network address.

    B. A MAC address is a unique host name.

    C. A MAC address is a unique hardware identifier.

    D. A MAC address is a unique alias.

23. 10.1.45.245 is an example of which of the following?

    A. A MAC address

    B. A host name

    C. An IP address

    D. An IP domain name

24. Code and databases are examples of which of the following?

    A. Software assets

    B. Proprietary information

    C. Internal-use classification

    D. Intellectual property (IP)

25. Which of the following terms best describes the act of classifying information based on an original classification decision already made by an authorized original classification authority?

    A. Reclassification

    B. Derivative classification

    C. Declassification

    D. Original classification

26. Which of the following types of information would not be considered NPPI?

    A. Social security number

    B. Date of birth

    C. Debit card PIN

    D. Home address

27. In keeping with best practices and regulatory expectations, legally protected data that is stored on mobile devices should be _____.

  - **A.** masked
  - **B.** encrypted
  - **C.** labeled
  - **D.** segregated

28. Which of the following statements best describes how written documents that contain NPPI should be handled?

  - **A.** Written documents that contain NPPI should be stored in locked areas or in a locked cabinet.
  - **B.** Written documents that contain NPPI should be destroyed by cross-cut shredding.
  - **C.** Written documents that contain NPPI should be subject to company retention policies.
  - **D.** All of the above.

29. Which of the following address types represents a device location on a network?

  - **A.** A physical address
  - **B.** A MAC address
  - **C.** A logical address
  - **D.** A static address

30. Which of the following statements is true?

  - **A.** Small businesses do *not* need to classify data because it is unusual for a small business to have NPPI.
  - **B.** Small businesses do *not* need to classify data because small businesses do not have regulatory obligations.
  - **C.** Small businesses need to classify data because small businesses are responsible for protecting NPPI, employee data, and company data.
  - **D.** Small businesses need to classify data because every organization is legally required to have a classification system.

EXERCISES

EXERCISE 5.1: Assigning Ownership

Owners are responsible for the protection of assets. For each of the following assets, assign an owner and list their responsibilities in regard to protecting the asset:

1. The house you live in.
2. The car you drive.
3. The computer you use.
4. The city you live in.

EXERCISE 5.2: Differentiating Between Ownership and Custodianship

A smartphone is an information system. As with any information system, data ownership and custodianship must be assigned.

1. If a company provides a smartphone to an employee to use for work-related communications:
   a. Who would you consider the information system owner? Why?
   b. Who would you consider the information system custodian? Why?
2. If a company allows an employee to use a personally owned device for work-related communications:
   a. Who would you consider the information system owner? Why?
   b. Who would you consider the information system custodian? Why?
   c. In regard to protecting data, should there be a distinction between company data and personal data?

EXERCISE 5.3: Creating an Inventory

You have been tasked with creating an inventory system for the computer lab at your school.

1. For the hardware in the lab, list at least five characteristics you will use to identify each asset.
2. For the software in the lab, list at least five characteristics you will use to identify each asset.
3. Create an inventory template. Use either a spreadsheet or database application.
4. Visit a classroom or lab and inventory a minimum of three hardware and three software assets.

EXERCISE 5.4: Reviewing a Declassified Document

Go to either http://FOIA.gov or the CIA FOIA Electronic Reading Room at www.foia.cia.gov.

1. Find a document that has been recently declassified.
2. Write a brief report explaining why and when the document was declassified.

EXERCISE 5.5: Understanding Color-Coded National Security

The Department of Homeland Security uses a color-coded advisory system to communicate threat levels to the public. This is an example of labeling.

1. What colors are used in the Threat Advisory System?
2. What does each of the colors mean?
3. Do you think these labels are an effective way to communicate threat information to the general public? Why or why not?

PROJECTS

PROJECT 5.1: Developing an Email Classification System and Handling Standards

Data classification categories and handling standards are necessary to properly protect information. Email is a good example of an information system that processes, stores, and transmits many different types of information.

1. Develop a three-level classification system for your email communications. Consider the type of emails you send and receive. Take into consideration who should be able to view, save, print, or forward your email. For each classification, decide how you will label your emails to communicate the assigned classification. For each classification, develop handling standards.
2. Multiple information systems are used to process, transmit, store, and back up email. Identify as many systems as possible involved in each step. For each system identified, document the person or position you would expect to be the information system owner. Is it necessary to provide them with a copy of your classification system or handling standards? Why or why not?
3. Sometimes information system owners have different priorities. For example, your Internet service provider (ISP) by law has the right to view/open all documents that are stored on or passed through its systems. The ISP may choose to exercise this right by scanning for viruses or checking for illegal content. Suppose you have sent emails that could cause you harm if they were disclosed or compromised. As the information owner, what are your options?

PROJECT 5.2: Classifying Your School Records

Over time, your school has accumulated a great deal of information about you and your family, including your medical records, finances (including tax returns), transcripts, and student demographic data (name, address, date of birth, and so on). It is important that access to this information be restricted to authorized users.

1. Create a table listing each of these information categories. Classify each one as either Protected, Confidential, Internal Use, or Public.
2. Include in your table a column defining the "Need to Know" criteria. (Hint: This is the reason someone should be granted access to the information.)
3. Even though the information pertains to you, you are not the owner. Include in your table a column listing who you would expect to be the information owner.
4. Choose one of the categories you have listed and find out where the information is actually stored, who is responsible for it, who has access to it, and what policies are in place to protect it. Compare this information with your answers to items 1, 2, and 3 of this project.

PROJECT 5.3: Locating and Using Special Publications

The National Institute of Standards and Technology (NIST) special publications contain a wealth of information applicable to both private and public sector organizations. In this exercise, you will familiarize yourself with locating and using special publications.

1. Download a copy of NIST SP 800-88, R1: Guidelines for Media Sanitization.
2. Read through the document.
3. To whom do they assign ultimate responsibility for media sanitization?
4. Refer to Figure 4-1, "Sanitization and Disposition Decision Flow." What is the relationship between this chart and classification levels?
5. In regard to media sanitization, explain the differences between clear, purge, and destroy?

Case Study

Assessing Classification and Authorization at SouthEast Healthcare

SouthEast Healthcare was founded in 1920. It is headquartered in Atlanta, Georgia and has 15 patient care sites located throughout the state. SouthEast Healthcare provides a full range of healthcare services. The organization is a leader in electronic medical records and telemedicine services delivered via the Web. Over the years, they have made significant information security investments, including advanced intrusion detection systems; programs that audit, monitor, and report access; biometric devices; and training. Although their information technology (IT) and security staff is small, they are a dedicated team of professionals. SouthEast Healthcare appeared to be a model of security and was selected to participate in a HIPAA security study. At first, the audit team was very impressed. Then they began to wonder how protection decisions were made. It appeared to them that all information assets were being treated with equal protection, which meant that some were perhaps protected too much whereas others were under-protected. They approached the CEO and asked her to explain how the organization made protection decisions. She replied that she left it up to the IT and security team. The auditors then went to the members of the team and asked them the same question. They enthusiastically replied that the importance of the various information assets was "institutional knowledge." They were puzzled when the auditors asked if the information owners classified the information and authorized the protection levels. No, they replied, it had always been left to them. The auditors were not happy with this answer and expressed their displeasure in their interim report. The auditors are coming back in three months to complete the study. SouthEast Healthcare's CEO wants this problem fixed before they return.

1. Who should take responsibility for the classification and authorization project?
2. Is this one project or two separate projects?
3. Who should be involved in this project(s)?
4. Would you engage external resources? Why or why not?
5. How would you gain consensus?
6. What involvement should the Board of Directors have?

References

Regulations Cited

FIPS PUB 199 Standards for the Security Categorization of Federal Information and Information Systems, February 2004, accessed 06/2013, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Freedom of Information Act, official website of the U.S. Department of Justice, FOIA, accessed 06/2013, www.foia.gov/.

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules 45 CFR Parts 160 and 164 Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule Federal Register, Volume 78, No. 17, January 25, 2013, accessed 06/2013, www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/.

United States Department of Defense Manual Number 52001.01, Volume 1, February 24, 2012, "Overview, Classification and Declassification," accessed 06/2013, www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf.

United States Department of Defense Manual Number 5200.01, Volume 2, March 19, 2013, “Marking of Classified Information,” accessed 06/2013, www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf.

United States Department of Agriculture, Personnel and Document Security Division, “Classification Guidelines and Distribution Controls, Original and Derivative,” accessed 06/2013, www.dm.usda.gov/ocpm/Security%20Guide/S1class/Classif.htm.

Executive Orders Cited

Executive Order 13526: Classified National Security Information. White House Office of the Press Secretary, December 29, 2009, accessed on 06/10/3013, www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information.

Other Research

Hosenball, Mark and Cowan (Reuters). “Edward Snowden, NSA Whistleblower, Says He Acted Out of Conscience to Protect ‘Basic Liberties,’” accessed on 06/10/2013, www.huffingtonpost.com/2013/06/10/edward-snowden-basic-liberties_n_3414824.html.

Radack, Shirley. “Risk Management Framework: Helping Organizations Implement Effective Information Security Programs,” NIST Computer Security Division, accessed 06/2013, http://csrc.nist.gov/publications/.../july2009_risk-management-framework.pdf.

Ross, Ron. “Risk Management Framework,” NIST Computer Security Division, accessed 06/2013, http:csrc.nist.gov/groups/SMA/fisma/.../risk-management-framework-2009.pdf.

Chapter 6

Human Resources Security

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Define the relationship between information security and personnel practices.
- Recognize the stages of the employee lifecycle.
- Describe the purpose of confidentiality and acceptable use agreements.
- Understand appropriate security education, training, and awareness programs.
- Create personnel-related security policies and procedures.

Is it possible that people are simultaneously an organization's most valuable asset and their most dangerous threat? Study after study cites people as the weakest link in information security. Because information security is primarily a people-driven process, it is imperative that the information security program be faithfully supported by information owners, custodians, and users.

For an organization to function, employees need access to information and information systems. Because we are exposing valuable assets, we must know our employees' background, education, and weaknesses. Employees must also know what is expected of them; from the very first contact, the organization needs to deliver the message that security is taken seriously. Conversely, candidates and employees provide employers with a great deal of personal information. It is the organization's responsibility to protect employee-related data in accordance with regulatory and contractual obligations.

Before employees are given access to information and information systems, they must understand organizational expectations, policies, handling standards, and consequences of noncompliance. This information is generally codified into two agreements: a confidentiality agreement and an acceptable use agreement. Acceptable use agreements should be reviewed and updated annually and redistributed to employees for signature. An orientation and training program should be designed to explain and expand upon the concepts presented in the agreements. Even long-standing employees continually need to be reeducated about security issues. NIST has invested significant resources in developing a role-based Security Education, Training, and Awareness (SETA) model. Although designed for government, the model is on target for the private sector.

We will begin this chapter with examining the security issues associated with employee recruitment, onboarding, user provisioning, career development, and termination. We will then discuss the importance of confidentiality and acceptable use agreements. Lastly, we will focus on the SETA training methodology. Throughout the chapter, we will codify best practices into human resources security policy.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 7 of ISO 27002:2013 is dedicated to Human Resources Security Management with the objective of ensuring that security is integrated into the employee lifecycle.

Corresponding NIST guidance is provided in the following documents:

- SP 800-12: An Introduction to Computer Security—The NIST Handbook
- SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model
- SP 800-50: Building an Information Technology Security Awareness and Training Program
- SP 800-100: Information Security Handbook: A Guide for Managers

The Employee Lifecycle

The ***employee lifecycle 1*** model (shown in Figure 6-1) represents stages in an employee's career. Specific employee lifecycle models vary from company to company but common stages include the following:

- **Recruitment**—This stage includes all the processes leading up to and including the hiring of a new employee.
- **Onboarding**—In this stage, the employee is added to the organization's payroll and benefits systems.
- **User provisioning**—In this stage, the employee is assigned equipment as well as physical and technical access permissions. The user provisioning process is also invoked whenever there is a change in the employee's position, level of access required, or termination.
- **Orientation**—In this stage, the employee settles into the job, integrates with the corporate culture, familiarizes himself with coworkers and management, and establishes his role within the organization.

- **Career development**—In this stage, the employee matures in his role in the organization. Professional development frequently means a change in roles and responsibilities.
- **Termination**—In this stage, the employee leaves the organization. The specific processes are somewhat dependent on whether the departure is the result of resignation, firing, or retirement. Tasks include removing the employee from the payroll and benefits system, recovering information assets such as his smartphone, and deleting or disabling user accounts and access permissions.

With the exception of career development, we are going to examine each of these stages in relation to information security concepts, safeguards, and policies.

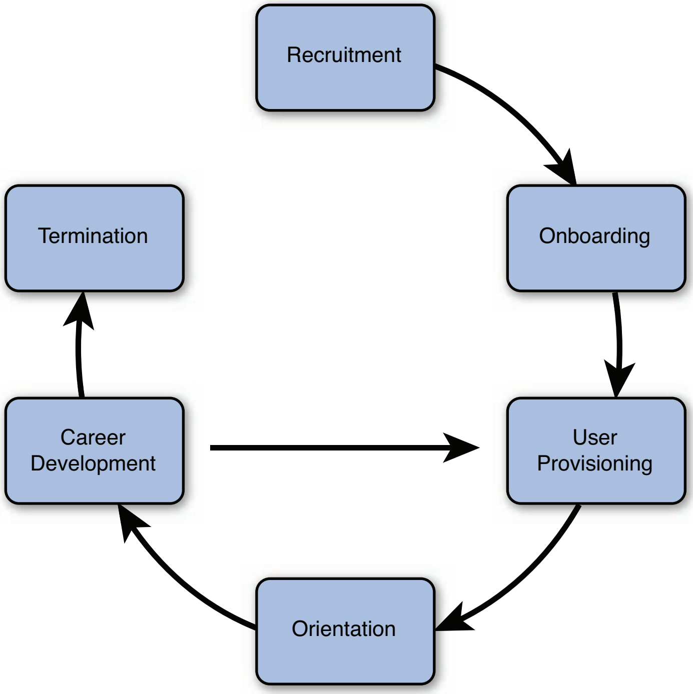


FIGURE 6.1 The employee lifecycle.

What Does Recruitment Have to Do with Security?

The recruitment stage includes developing and publishing job descriptions, actively seeking potential employees, collecting and assessing candidate data, interviewing, conducting background checks, and either making an offer or rejecting a candidate. A significant flow of information occurs during the recruitment stage. In hopes of attracting the most qualified candidate, information about the organization is publicly revealed. In turn, potential candidates respond with a plethora of personal information.

Job Postings

The first direct contact many potential candidates have with their future employer is a help-wanted advertisement. Historically, this advertisement was either published in a newspaper or trade journal or provided to a "headhunter" who specialized in finding potential candidates. In either case, the circulation was limited in scope and time. Today, a majority of recruiting is Internet-based. Companies may post jobs on their website, use online employment search engines such as Monster.com, or use social media such as LinkedIn. The upside to this trend is reaching a wider audience of talent. The downside is that this exposure also reaches a wider audience of potential intruders and may have the unintended consequence of exposing information about an organization. Job postings are one of the sources that intruders often look to use. Why? Because job postings can be a wealth of information about an organization: personnel changes, product development, new services, opening of offices, as well as basic information such as the name and phone number of the hiring manager. All of these items can be used in social engineering attacks and provide a path to more in-depth knowledge. An idea to consider is having two versions of a job description. Version A is posted and/or published and has enough information to attract the attention and interest of a potential employee. Version B is more detailed and is posted internally and/or shared with candidates that have made the "first cut." Version B of a job description needs to be detailed enough to convey the facets of the position and has the following characteristics:

- It conveys the mission of the organization.
- It describes the position in general terms.
- It outlines the responsibilities of the position.
- It details the necessary skill set.
- It states the organization's expectations regarding confidentiality, safety, and security. The goal of this characteristic is to deliver the message that the organization has a commitment to security and that all employees are required to honor that commitment.

What should not be in either version of the job description is information regarding specific systems, software versions, security configurations, or access controls.

Candidate Application Data

The intent of posting a job is to have candidates respond with pertinent information. Collecting candidate data is a double-edge sword. On one hand, companies need personal information to properly select potential employees. On the other hand, once this information is collected, companies are responsible for protecting the data as well as the privacy of the job seeker. ***Candidate data*** generally collected during this phase includes demographic, contact, work history, accomplishments, education, compensation, previous employer feedback, references, clearances, and certifications. If possible, legally protected ***non-public personal information*** (NPPI) such as social security number, date of birth, driver's license or state identification number, and financial information should not be collected at this stage.

FYI: Protecting Candidate Data

Companies have an obligation to protect the information provided by job seekers. The General Electric (GE) Candidate Data Protection Standards is a good example of how multinational companies approach the handling of candidate data. The "Principles for Processing Candidate Data" is listed here. The complete standard, which includes scope, application of local laws, data collection, purposes and access for candidate data processing, type of candidate data, security and confidentiality, rights of candidates, transferring data, direct marketing, enforcement rights and mechanisms, audit procedures, and standards modification, is published on the GE website (www.ge.com/careers/privacy). The principles for processing candidate data are as follows:

"GE respects the privacy rights and interests of each individual. GE entities will observe the following principles when processing Candidate Data:

- "Data will be processed fairly and lawfully.
- "Data will be collected for specified, legitimate purposes and not processed further in ways incompatible with those purposes.
- "Data will be relevant to and not excessive for the purposes for which they are collected and used. For example, Data may be rendered anonymous when feasible and appropriate, depending on the nature of the Data and the risks associated with the intended uses.
- "Data will be accurate and, where necessary, kept up-to-date. Reasonable steps will be taken to rectify or delete Candidate Data that is inaccurate or incomplete.
- "Data will be kept only as long as it is necessary for the purposes for which it was collected and processed.
- "Data will be processed in accordance with the individual's legal rights (as described in these Standards or as provided by law).
- "Appropriate technical, physical, and organizational measures will be taken to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to Data."

The Interview

Top-tier candidates are often invited to one or more interviews with a cross-section of personnel. Invariably, interviewers share more information than they should with job candidates. They do so for a variety of reasons. Sometimes they are trying to impress a sought-after candidate. They may be proud of (or dismayed with) the organization. Sometimes they simply do not realize the confidentiality of the information they are sharing. For example, an interviewer might reveal that the organization is about to launch a new mobile app and that they know little about how to secure it! Creating and following an interview script (that has been vetted by information security personnel) can minimize the risk of disclosure. One of the worst mistakes that an interviewer can make is taking an early-stage job candidate on a tour of the facility. A candidate should never be allowed access to secure areas without prior authorization by the information system owner. Even then, caution should be taken.

In Practice

Job Recruitment Policy

Synopsis: In support of information security, the purpose of this policy is to ensure that company and candidate resources are protected during the recruitment process.

Policy Statement:

- Any information that is classified as “protected” or “confidential” must *not* be included in job postings or job descriptions.
- Candidates will not be allowed access to any secure area unless authorized in writing by the information owner.
- All nonpublic information submitted by candidates must be classified as “protected” and handled in accordance with company handling standards.
- Under no circumstances will the company request that candidates provide a password to social media, blog, web, or personal email accounts.
- The Office of Information Security and the Office of Human Resources will be jointly responsible for the implementation and enforcement of this policy.

Screening Prospective Employees

You are a business owner. You have spent the last ten years toiling night and day to build your business. You have invested your personal financial resources. Your reputation in the community is intertwined with the actions of the business. How much do you need to know about your newest salesperson?

You are the Chief Executive Officer (CEO) of a Fortune 1000 financial services company. You are responsible to the stockholders and accountable to the government for the actions of your business. How much do you need to know about your new Chief Financial Officer (CFO)?

You are the Head of Medicine at your local hospital. You are responsible for maintaining the health of your patients and for guaranteeing their right to privacy. How much do you need to know about the new emergency room intake nurse?

In all three cases, the information owner wants assurance that the user will treat the information appropriately in accordance with its classification. One of the standards in determining who should have access is defining the user criteria. These criteria extend to their background: education, experience, certification/license, criminal record, and financial status. In addition, we must consider the amount of power or influence the employee will have in the organization.

For example, we expect that a CFO will have access to confidential financial records and sensitive corporate strategy documents. In addition, the CFO has the power to potentially manipulate the data. In this case, we need to be concerned about both the confidentiality and the integrity of the information.

It seems obvious that the CFO needs to be held to a high standard. He should have a spotless criminal record and not be under any financial pressure that may lead to inappropriate activities such as embezzlement. Unfortunately, as corporate scandals such as Enron, Adelphia, HealthSouth, and Tyco have shown us, those in power do not always act in the best interest of the organization. The organization needs to proactively protect itself by conducting background and reference checks on potential employees and directors. The same holds true for positions of less prominence, such as a salesperson or intake nurse. Although these positions may have less power, the potential for misuse still exists.

FYI: Sarbanes-Oxley Act (SOX): A Response to Misuse of Power

"On July 30, 2002, President Bush signed into law the Sarbanes-Oxley Act of 2002, which he characterized as 'the most far reaching reforms of American business practices since the time of Franklin Delano Roosevelt.' The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud, and created the 'Public Company Accounting Oversight Board,' also known as the PCAOB, to oversee the activities of the auditing profession."

The full text of the Act is available at www.sec.gov/about/laws/soa2002.pdf. You can find links to all commission rulemaking and reports issued under the Sarbanes-Oxley Act at www.sec.gov/spotlight/sarbanes-oxley.htm.

Not all potential employees need to undergo the same level of scrutiny. It is the responsibility of the information owner to set standards based on level of information access and position. It is important to have a policy that sets the minimum standards for the organization yet affords information owners the latitude to require additional or more in-depth background checks or investigations. This is an example of a policy that in the development stage may need to involve outsiders such as legal counsel or employee representatives. Many organizations have union labor. The union contract may forbid the background checks. This policy would need to be incorporated into the next round of negotiations.

The following are rules you should be aware of:

- **Workers' right to privacy**—There are legal limits on the information you can gather and use when making employment decisions. Workers have a right to privacy in certain personal matters, a right they can enforce by suing you if you pry too deeply. Make sure your inquiries are related to the job. Stick to information that is relevant to the job for which you are considering the worker.
- **Getting consent**—Although not universally required by law, conventional wisdom recommends asking candidates to agree to a background check. Most organizations include this request on their application forms and require the applicant to agree in writing. By law, if a candidate refuses to agree to a reasonable request for information, you may decide not to hire the worker on that basis.
- **Using social media**—Social media sites are increasingly being used to "learn more" about a candidate. In 2011, social media monitoring service Reppler surveyed more than 300

hiring professionals to determine when and how job recruiters are screening job candidates on different social networks. The study found that more than 90% of recruiters and hiring managers have visited a potential candidate's profile on a social network as part of the screening process. Social media profiles include information such as gender, race, and religious affiliation. The law prohibits the use of this information for hiring. Access to this info could have the organization subject to discrimination charges. Legal experts recommend that organizations have a non-decision maker conduct the search and provide to the decision maker(s) only relevant job-related information.

- **Educational records**—Under the ***Family Educational Rights and Privacy Act (FERPA)***, schools must have written permission in order to release any information from a student's education record. For more information on obtaining records under FERPA, go to www.ed.gov.
- **Motor vehicle records**—Under the federal ***Drivers Privacy Protection Act (DPPA)***, the release or use by any state DMV (or any officer, employee, or contractor thereof) of personal information about an individual obtained by the department in connection with a motor vehicle record is prohibited. The latest amendment to the DPPA requires states to get permission from individuals before their personal motor vehicle record may be sold or released to third-party marketers.
- **Financial history**—According to the Federal Trade Commission (FTC), you may use credit reports when you hire new employees and when you evaluate employees for promotion, reassignment, and retention—as long as you comply with the ***Fair Credit Reporting Act (FCRA)***. Sections 604, 606, and 615 of the FCRA spell out employer responsibilities when using credit reports for employment purposes. These responsibilities include the requirement of notification if the information obtained may result in a negative employment decision. The ***Fair and Accurate Credit Transaction Act of 2003 (FACTA)*** added new sections to the federal FCRA, intended primarily to help consumers fight the growing crime of identity theft. Accuracy, privacy, limits on information sharing, and new consumer rights to disclosure are included in FACTA. For more information on using credit reports and the FCRA, go to www.ftc.gov.
- **Bankruptcies**—Under ***Title 11 of the U.S. Bankruptcy Code***, employers are prohibited from discriminating against someone who has filed for bankruptcy. Although employers can use a negative credit history as a reason not to hire, employers cannot use bankruptcy as a sole reason.
- **Criminal record**—The law on how this information can be used varies extensively from state to state.
- **Workers' Compensation history**—In most states, when an employee's claim goes through Workers' Compensation, the case becomes public record. An employer may only use this information if an injury might interfere with one's ability to perform required duties. Under the federal ***Americans with Disabilities Act***, employers cannot use medical information or the fact an applicant filed a Workers' Compensation claim to discriminate against applicants.

Table 6.1 describes the various types of background checks.

TABLE 6.1 Types of Background Checks

Check Type	Description
Educational	Verification that all educational credentials listed on the application, resume, or cover letter are valid and have been awarded.
Employment	Verification of all relevant previous employment as listed on the application, resume, or cover letter.
License/certification	Verification of all relevant licenses, certifications, or credentials.
Credit history	Checking the credit history of the selected applicant or employee. Federal laws prohibit discrimination against an applicant or employee because of bankruptcy. Federal law also requires that applicants be notified if their credit history influences the employment decision.
Criminal history	Verification that the selected applicant or employee does not have any undisclosed criminal history.

In Practice

Personnel Screening Policy

Synopsis: Background checks must be conducted on employees, temporaries, and contractors.

Policy Statement:

- As a condition of employment, all employees, temporaries, and contractors must agree to and are subject to background screening that includes identity verification, confirmation of educational and professional credentials, credit check, and state and federal criminal check.
- Comprehensive background screening will be conducted pre-hire. Criminal check will be conducted annually thereafter.
- Background screening will be conducted in accordance with local, state, and federal law and regulations.
- If the person will have access to “protected” or highly confidential information, additional screening may be required at the discretion of the information owner. This includes new personnel as well as employees who might be moved into such a position.
- Background screening will be conducted and/or managed by the Human Resources department.

- If temporary or contractor staff is provided by an agency or third party, the contract must clearly specify the agency or third-party responsibility for conducting background checks in accordance with this policy. Results must be submitted to the Human Resources department for approval.
- The Office of the Information Security Office and the Office of Human Resources will be jointly responsible for the implementation and enforcement of this policy.
- All information obtained in the screening process will be classified as "protected" and handled in accordance with company handling standards.

Government Clearance

Many U.S. government jobs require that the prospective employee have the requisite security clearance. Although each government agency has its own standards, in general, a ***security clearance*** investigation is an inquiry into an individual's loyalty, character, trustworthiness, and reliability to ensure that he or she is eligible for access to national security–related information. The process to obtain clearance is both costly and time consuming. The four-phase process includes the following stages:

1. **Application phase**—This phase includes verification of U.S. citizenship, fingerprinting, and completion of the Personnel Security Questionnaire (SF-86).
2. **Investigative phase**—This phase includes a comprehensive background check.
3. **Adjudication phase**—During this phase, the findings from the investigation are reviewed and evaluated based on 13 factors determined by the Department of Defense. Examples of these factors include criminal and personal conduct, substance abuse, and any mental disorders.
4. **Granting (or denial) of clearance at a specific level**—In order to obtain access to data, clearance and classification must match. For example, in order to view Top Secret information, the person must hold Top Secret clearance. However, merely having a certain level of security clearance does not mean one is authorized to access the information. To have access to the information, one must possess two elements: a level of security clearance, at least equal to the classification of the information, and an appropriate "need to know" the information in order to perform their duties.

What Happens in the Onboarding Phase?

Once hired, a candidate transitions from a potential hire to an employee. At this stage, he or she is added to the organization's payroll and benefits systems. In order to accomplish these tasks, the employee must provide a full spectrum of personal information. It is the responsibility of the organization to properly classify and safeguard employee data.

Payroll and Benefits Employee Data

When an employee is hired in the United States, he or she must provide proof of identity, work authorization, and tax identification. The two forms that must be completed are the Department of Homeland Security/U.S. Citizenship and Immigration Services Form I-9 Employment Eligibility Verification and the Internal Revenue Service Form W-4 Employee's Withholding Allowance Certificate.

The purpose of Form I-9 is to prove that each new employee (both citizen and noncitizen) is authorized to work in the United States. Employees are required to provide documentation that (a) establishes both identity and employment authorization *or* (b) documents and establishes identity *and* (c) documents and establishes employment authorization. Employees provide original documentation to the employer, who then copies the documents, retains a copy, and returns the original to the employee. Employers who hire undocumented workers are subject to civil and criminal penalties per the Immigration Reform and Control Act of 1986. For an example of an I-9 form, visit www.uscis.gov/sites/default/files/files/form/i-9.pdf. As shown on page 9 of this document, the required documents may contain NPPI and must be safeguarded by the employer.

Completion of Form W-4 is required in order for employers to withhold the correct amount of income tax from employee pay. Information on this form includes complete address, marital status, social security number, and number of exemptions. Additionally, according to the W-4 Privacy Act Notice, routine uses of this information include giving it to the Department of Justice for civil and criminal litigation; to cities, states, the District of Columbia, and U.S. commonwealths and possessions for use in administering their tax laws; and to the Department of Health and Human Services for use in the National Directory of New Hires. They may also disclose this information to other countries under a tax treaty, to federal and state agencies to enforce federal nontax criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. The confidentiality of information provided on Form W-4 is legally protected under 26 USC § 6103: Confidentiality and Disclosure of Returns and Return Information.

What Is User Provisioning?

User provisioning is the name given to the process of creating user accounts and group membership, providing company identification, assigning access rights and permissions as well as access devices such as a token or smartcard. This process may be manual, automated (commonly referred to as an identity management system), or a combination thereof. Prior to granting access, the user should be provided with and acknowledge the terms and conditions of an acceptable use agreement. We will examine this agreement later in the chapter. The permissions and access rights a user is granted should match his or her role and responsibilities. The information owner is responsible for defining who should be granted access and under what circumstances. Supervisors generally request access on behalf of their employees. Depending on the organization, the provisioning process is managed by the Human Resources department, the Information Security department, or the Information Technology (IT) department. We will discuss role-based access controls later in the book.

In Practice

User Provisioning Policy

Synopsis: The company must have an enterprise-wide user provisioning process.

Policy Statement:

- There will be defined and documented a user provisioning process for granting and revoking access to information resources that includes but is not limited to account creation, account management (including assignment of access rights and permissions), periodic review of access rights and permissions, and account termination.
- The Office of Human Resources and the Office of Information Security are jointly responsible for the user provisioning process.

What Should an Employee Learn During Orientation?

In this stage, the employee begins to learn about the company, the job, and coworkers. Before having access to information systems, it is important that the employee understand his or her responsibilities, learn the information-handling standards and privacy protocols, and have an opportunity to ask questions. Organizational orientation is usually a Human Resources department responsibility. Departmental orientation is usually conducted by a supervisor or departmental trainer. Employee orientation training is just the beginning. Every employee should participate in SETA programs throughout his or her tenure. We'll examine the importance of SETA later in this chapter.

Privacy Rights

The standard in most private sector organizations is that employees should have *no expectation of privacy* in respect to actions taken on company time or with company resources. This extends to electronic monitoring, camera monitoring, and personal searches.

- Electronic monitoring includes phone, computer, email, mobile, text, Internet access, and location (GPS-enabled devices).
- Camera monitoring includes on-premise locations, with the exception of cameras in restrooms or locker rooms where employees change clothes, which is prohibited by law.
- Personal searches extend to searching an employee, an employee's workspace, or an employee's property, including a car, if it is on company property. Personal searches must be conducted in accordance with state regulations.

A company should disclose its monitoring activities to employees and get written acknowledgment of the policy. According to the American Bar Association, "an employer that fails to adopt policies or warnings or acts inconsistently with its policies or warnings may find that the employee still has a reasonable expectation of privacy." The lesson is that companies must have clear policies and be consistent in their application. Privacy expectations should be defined in the information security policy, acknowledged in the signed acceptable use agreement, and included in login banners and warnings.

In Practice

Electronic Monitoring Policy

Synopsis: It is necessary to have the ability to monitor certain employee activities. Employee expectation of privacy must be clearly defined and communicated.

Policy Statement:

- The company reserves the right to monitor electronic activity on company-owned information systems, including but not limited to voice, email, text and messaging communications sent, received, or stored, computer and network activity, and Internet activity, including sites visited and actions taken.
- The policy must be included in the employee acceptable use agreement, and employees must acknowledge the policy by signing the agreement.
- Whenever technically feasible, login banners and warning messages will remind users of this policy.
- The Office of Human Resources and the Office of Information Security are jointly responsible for developing and managing electronic monitoring and employee notification.

Why Is Termination Considered the Most Dangerous Phase?

In this stage, the employee leaves the organization. This is an emotionally charged event. Depending on the circumstances, the terminated employee may seek revenge, create havoc, or take information with him. Don't assume that a termination is friendly even if the employee resigns for personal reasons or is retiring. A 2009 Ponemon Institute survey of 945 individuals who were laid off, fired, or quit their jobs within the previous 12 months shows that 59% admitted to stealing confidential company information, such as customer contact lists, email lists, employee records, customer information and contact lists, and non-financial information, and 67% used their former company's confidential information to leverage a new job. The survey also found that 53% of respondents downloaded information onto a CD or DVD; 42% downloaded data onto a USB drive; and 38% sent attachments to a personal email account.

How termination is handled depends on the specific circumstances and transition arrangements that have been made with the employee. However, in situations where there is any concern that an employee may react negatively to being terminated or laid off, access to the network, internal, and web-based application, email, and company owned social media should be disabled prior to informing the employee. Similarly, if there is any cause for concern associated with a resignation or retirement, all access should be disabled. If the employee is leaving to work at a competitor, best bet is to escort them off the property immediately. In all cases, make sure not to forget about remote access capabilities.

FYI: The Case of the Disgruntled Ex-Network Administrator

Danielle Duann (51) of Houston, Texas, pleaded guilty on April 30, 2009 to a criminal indictment charging her with unauthorized computer access. In addition to a two-year prison term, Duann was sentenced to a three-year period of supervised release following completion of her prison sentence, and ordered to pay $94,222 in restitution to compensate her former employer for the damage that resulted from her actions.

In pleading guilty, Duann admitted to illegally accessing the computer network of LifeGift Organ Donation Center and then intentionally deleting organ donation database records, accounting invoice files, database and accounting software applications, and various backup files, without authorization. LifeGift is the sole provider of organ procurement services for more than 200 hospitals throughout 109 counties in North, Southeast, and West Texas.

According to court documents, LifeGift terminated Duann from her position as their director of IT on November 7, 2005 and revoked all of her previous administrative rights and access to the LifeGift computer network. In pleading guilty, Duann admitted that beginning on the evening of November 7, 2005 and continuing until November 8, 2005, she repeatedly gained unauthorized access to the LifeGift computer network via a remote connection from her home and intentionally caused damage by deleting numerous database files and software applications, as well as their backups, related to LifeGift's organ and tissue recovery operations.

Duann further admitted that in an attempt to conceal her activities, she disabled the computer logging functions on several LifeGift computer servers and erased the computer logs that recorded her remote access to the LifeGift network.

This case was investigated by the FBI and was prosecuted by the Department of Justice.

In Practice

Employee Termination Policy

Synopsis: Information assets and systems must be protected from terminated employees.

Policy Statement:

- Upon the termination of the relationship between the company and any employee, all access to facilities and information resources shall cease.
  - In the case of unfriendly termination, all physical and technical access will be disabled pre-notification.
  - In the case of a friendly termination, including retirement, the Office of Human Resources is responsible for determining the schedule for disabling access.
- Termination procedures are to be included in the user provisioning process.
- The Office of Human Resources and the Office of Information Security are jointly responsible for the user provisioning process.

The Importance of Employee Agreements

It is common practice to require employees, contractors, and outsourcers to sign two basic agreements: a confidentiality agreement (also known as a *non-disclosure agreement*) and an acceptable use agreement. Confidentiality agreements are in place to protect from unauthorized disclosure of information and are generally a condition of work, regardless of access to information systems. Acceptable use agreements traditionally focus on the proper use of information systems and cover such topics as password management, Internet access, remote access, and handling standards. A growing trend is to augment the agreement-distribution process with training and explanation; the ultimate goal of the acceptable use agreement is to teach the employee the importance of security, obtain commitment, and install organizational values.

What Are Confidentiality or Non-disclosure Agreements?

Confidentiality or non-disclosure agreements are contracts entered into by the employee and the organization in which the parties agree that certain types of information remain confidential. The type of information that can be included is virtually unlimited. Any information can be considered confidential—data, expertise, prototypes, engineering drawings, computer software, test results, tools, systems, and specifications.

Confidentiality agreements perform several functions. First and most obviously, they protect confidential, technical, or commercial information from disclosure to others. Second, they can prevent the forfeiture of valuable patent rights. Under U.S. law and in other countries as well, the public disclosure of an invention can be deemed as a forfeiture of patent rights in that invention. Third, confidentiality agreements define exactly what information can and cannot be disclosed. This is usually accomplished by specifically classifying the information as such and then labeling it appropriately (and clearly). Fourth, confidentiality agreements define how the information is to be handled and for what length of time. Last, they state what is to happen to the information when employment is terminated or, in the case of a third party, when a contract or project ends.

What Is an Acceptable Use Agreement?

An ***acceptable use agreement*** is a policy contract between the company and information systems user. By signing the agreement, the user acknowledges and agrees to the rule regarding how he or she must interact with information systems and handle information. It is also a teaching document that should reinforce the importance of information security to the organization. Another way to think about an acceptable use agreement is that it is a condensed version of the entire information security policy document specifically crafted for employees. It contains only the policies and standards that pertain to them and is written in language that can be easily and unequivocally understood. A sample acceptable use agreement can be found in Appendix C, "Information Systems Acceptable Use Agreement and Policy."

Components of an Acceptable Use Agreement

An acceptable use agreement should include an introduction, information classifications, categorized policy statements, data-handling standards, sanctions for violations, contacts, and an employee acknowledgment:

- The *introduction* sets the tone for the agreement and emphasizes the commitment of the leadership of the organization.
- *Data classifications* define (and include examples of) the classification schema adopted by the organization.
- *Applicable policy statements* include Authentications & Password Controls, Application Security, Messaging Security (including email, instant message, text, and video conferencing), Internet Access Security, Remote Access Security, Mobile Device Security, Physical Access Security, Social Media, Incident Use of Information Resources, Expectation of Privacy, and Termination.
- *Handling standards* dictate by classification level how information must be stored, transmitted, communicated, accessed, retained, and destroyed.
- *Contacts* should include to whom to address questions, report suspected security incidents, and report security violations.
- The Sanctions for Violations section details the internal process for violation as well as applicable civil and criminal penalties for which the employee could be liable.
- The *Acknowledgment* states that the user has read the agreement, understands the agreement and the consequences of violation, and agrees to abide by the policies presented. The agreement should be dated, signed, and included in the employee permanent record.

In Practice

Employee Agreements Policy

Synopsis: All employees and third-party personnel not otherwise covered by contractual agreement are required to agree to Confidentiality and Acceptable Use requirements.

Policy Statement:

- All employees must be provided with and sign a confidentiality agreement as a condition of employment and prior to being provided any company information classified as protected, confidential, or internal use.
- All employees must be provided with and sign an acceptable use agreement as a condition of employment and prior to being granted access to any company information or systems.
- The documents provided to the employee will clearly state the employees' responsibilities during both employment and post-employment.

- The employee's legal rights and responsibilities will be included in the document.
- Legal counsel is responsible for developing, maintaining, and updating the confidentiality agreement.
- The Office of Information Security is responsible for developing, maintaining, and updating the acceptable use agreement.
- The Office of Human Resources is responsible for distributing the agreement and managing the acknowledgment process.

The Importance of Security Education and Training

NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program succinctly defines why security education and training is so important:

"Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment without ensuring that all people involved in using and managing IT:

- "Understand their roles and responsibilities related to the organizational mission;
- "Understand the organization's IT security policy, procedures, and practices;
- "Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

"The 'people factor'—not technology—is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this 'asset.'

"A strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. In addition, those in the agency who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to the area of security training puts an enterprise at great risk because security of agency resources is as much a *human issue* as it is a technology issue.

"Everyone has a role to play in the success of a security awareness and training program, but agency heads, Chief Information Officers (CIOs), program officials, and IT security program managers have key responsibilities to ensure that an effective program is established agency wide. The scope and content of the program must be tied to existing security program directives and established agency security policy. Within agency IT security program policy, there must exist clear requirements for the awareness and training program."

What Is the SETA Model?

The term *security education* is really a catchall for three different programs: security education, training, and awareness. NIST SP 800-16 refers to this as the ***SETA model*** and assigns specific attributes to each program. Table 6.2 shows the NIST SP 800-16 SETA model.

TABLE 6.2 NIST SP 800-16 SETA Model

Security	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Awareness
Teaching Method	Discussion, seminar, reading	Lecture, case study, hands on	Interactive, video, posters, games
Test Measure	Essay	Problem solving	True or false, multiple choice
Impact Timeframe	Long-term	Intermediate	Short term

In times of corporate prosperity, SETA is often well funded. Unfortunately, the opposite is true as well. In times of economic downturn, these programs are scaled back or eliminated. That is a mistake. In hard times, there is even more temptation for industrial espionage, embezzlement, and thievery. This is the time information assets need the most protection. One way to ensure the continuation of SETA programs is to codify their importance in policy. The policy makers in Washington, D.C. understood this reality and included training and security awareness requirements in a number of privacy and security regulations, including FACTA, DPPA, FISMA, and HIPAA.

FYI: HIPAA Security Awareness and Training Requirement

Although many regulations require security awareness training, HIPAA is unique in that it explicitly specifies the topics to be covered. HIPAA Section 164.308(a)(5) Security Awareness and Training states that covered entities must “implement a security awareness and training program for all members of its workforce (including management).” The requirement includes four implementation standards:

- Security reminders
- Protection from malicious software
- Log-in monitoring
- Password management

In addition, periodic retraining is required whenever environmental or operational changes affect the security of protected health information. Changes may include new or updated policies and procedures, new or upgraded software or hardware, new security technology, or even changes in the Security Rule. Covered entities must document their security awareness and training programs, including on-going security reminders.

Influencing Behavior with Security Awareness

Security awareness is defined in NIST Special Publication 800-16 as follows: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly." *Security awareness* programs are designed to remind the user of appropriate behaviors. In our busy world, sometimes it is easy to forget why certain controls are in place. For example, an organization may have access control locks to secure areas. Access is granted by entering a PIN on the lock pad or perhaps using a swipe card. If the door doesn't click shut or someone enters at the same time, the control is effectively defeated. A poster reminding us to check and make sure the door is shut completely is an example of an awareness program.

Teaching a Skill with Security Training

Security training is defined in NIST Special Publication 800-16 as follows: "Training seeks to teach skills, which allow a person to perform a specific function." Examples of training include teaching a system administrator how to create user accounts, training a firewall administrator how to close ports, or training an auditor how to read logs. Training is generally attended by those tasked with implementing and monitoring security controls. You may recall from previous chapters that the person charged with implementing and maintaining security controls is referred to as the ***information custodian***.

Security Education Is Knowledge Driven

Security education is defined in NIST Special Publication 800-16 as follows: "The 'Education' level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response."

Education is management-oriented. In the field of information security, education is generally targeted to those who are involved in the decision-making process: classifying information, choosing controls, and evaluating and reevaluating security strategies. The person charged with these responsibilities is often the information owner.

In Practice

Information Security Training Policy

Synopsis: All employees, contractors, interns, and designated third parties must receive training appropriate to their position throughout their tenure.

Policy Statement:

- The Human Resources department is responsible for information security training during the employee orientation phase. The training must include compliance requirements, company policies, and handling standards.
- Subsequent training will be conducted at the departmental level. Users will be trained on the use of departmental systems appropriate to their specific duties to ensure that the confidentiality, integrity, and availability (CIA) of information is safeguarded.
- Annual information security training will be conducted by the Office of Information Security. All staff is required to participate and attendance will be documented. At a minimum, training will include the following topics: current information security–related threats and risks, security policy updates, and reporting of security incidents.
- The company will support the ongoing education of information security personnel by funding attendance at conferences, tuition at local colleges and universities, subscriptions to professional journals, and membership in professional organizations.

FYI: Small Business Note

Many small businesses treat employees like family. They are uncomfortable with the idea of background checks, confidentiality agreements, or acceptable use agreements. They don’t want to give the impression that their employees are not trusted. Small business owners need to recognize human resources security practices as positive safeguards designed to protect the long-term health of the company and, in turn, their employees.

Background verification, confidentiality agreements, and acceptable use agreements may be even more important in small organizations than a large one. Small business employees often wear many hats and have access to a wide range of company information and system. Misuse, disclosure, or actions that result in compromise or exposure could easily devastate a small business. Small businesses don’t have to go it alone. A number of reputable and affordable third-party service providers can assist with recruiting, conduct background checks, and craft appropriate agreements on behalf of the organization.

Summary

Personnel security needs to be embedded in each stage of the employee lifecycle—recruitment, onboarding, user provisioning, orientation, career development, and termination. It is the responsibility of the organization to deliver the message that security is a priority even before an employee joins the organization. Job postings, job descriptions, and even the interview process need to reflect an organizational culture committed to information security. Most importantly, companies need to protect candidate data, including NPPI, demographics, work history, accomplishments, education, compensation, previous employer feedback, references, clearances, and certifications. If the candidate is hired, the obligation extends to employee information.

Prior to hire, candidates should be subject to background checks, which may include criminal record, credit record, and licensure verification. Employers should request consent prior to conducting background checks. There are legal limits on the information that can be used to make employment decisions. Rules to be aware of include worker's right to privacy, social media restrictions, and regulatory restraints related to credit, bankruptcy, workers compensation and medical information.

Many U.S. government jobs require that the prospective employee have the requisite security clearance and in addition to the standard screening will investigate an individual's loyalty, character, trustworthiness, and reliability to ensure that he or she is eligible for access to national security–related information.

Confidentiality and acceptable use agreements should be a condition of employment. A *confidentiality agreement* is a legally binding obligation that defines what information can be disclosed, to whom, and within what time frame.

An *acceptable use agreement* is an acknowledgment of organization policy and expectations. An acceptable use agreement should include information classifications, categorized policy statements, data-handling standards, sanctions for violations, and contact information for questions. The agreement should disclose and clearly explain the organization's privacy policy and the extent of monitoring the employee should expect. Training and written acknowledgment of rights and responsibilities should occur prior to being granted access to information and information systems. Organizations will reap significant benefits from training users throughout their tenure. Security awareness programs, security training, and security education all serve to reinforce the message that security is important. Security awareness programs are designed to remind the user of appropriate behaviors. Security training teaches specific skills. Security education is the basis of decision making.

From a security perspective, termination is fraught with danger. How termination is handled depends on the specific circumstances and transition arrangements that have been made with the employee. Regardless of the circumstance, organizations should err on the side of caution and disable or remove network, internal, web-based application, email, and company-owned social media rights as soon as possible.

Human Resources policies include job recruitment, personnel screening, employee agreements, user provisioning, electronic monitoring, information security training, and employee termination.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following statements best describes the employee lifecycle?

   A. The employee lifecycle spans recruitment to career development.

   B. The employee lifecycle spans onboarding to orientation.

   C. The employee lifecycle spans user provision to termination.

   D. The employee lifecycle spans recruitment to termination.

2. At which of the following phases of the hiring process should personnel security practices begin?

   A. Interview

   B. Offer

   C. Recruitment

   D. Orientation

3. A published job description for a web designer should not include which of the following?

   A. Job title

   B. Salary range

   C. Specifics about the web development tool the company is using

   D. Company location

4. Data submitted by potential candidates must be ____________.

   A. protected as required by applicable law and organizational policy

   B. not protected unless the candidate is hired

   C. stored only in paper form

   D. publicly accessible

5. During the course of an interview, a job candidate should be given a tour of which of the following locations?

   A. The entire facility

   B. Public areas only (unless otherwise authorized)

   C. The server room

   D. The wiring closet

6. Which of the following facts is an interviewer permitted to reveal to a job candidate?
   - A. A detailed client list
   - B. The home phone numbers of senior management
   - C. The organization's security weaknesses
   - D. The duties and responsibilities of the position

7. Which of the following statements best describes the reason for conducting background checks?
   - A. To verify the truthfulness, reliability, and trustworthiness of the applicant
   - B. To find out if the applicant ever got in trouble in high school
   - C. To find out if the applicant has a significant other
   - D. To verify the applicant's hobbies, number of children, and type of house

8. Which of the following statements best describes the background check criteria?
   - A. Criteria should be the same for all prospective employees.
   - B. Criteria should differ according to gender or ethnicity.
   - C. Criteria should be specific to the job for which an applicant is applying.
   - D. None of the above.

9. Social media profiles often include gender, race, and religious affiliation. Which of the following statements best describes how this information should be used in the hiring process?
   - A. Gender, race, and religious affiliation can legally be used in making hiring decisions.
   - B. Gender, race, and religious affiliation cannot legally be used in making hiring decisions.
   - C. Gender, race, and religious affiliation are useful in making hiring decisions.
   - D. Gender, race, and religious affiliation listed in social media profiles should not be relied upon as they may be false.

10. Under the Fair Credit Reporting Act (FCRA), which of the following statements is true?
    - A. Employers cannot request a copy of an employee's credit report under any circumstances.
    - B. Employers must get the candidate's consent to request a credit report.
    - C. Employers cannot use credit information to deny a job.
    - D. Employers are required to conduct credit checks on all applicants.

11. Candidate and employee NPPI must be protected. NPPI does not include which of the following?

    A. Social security number

    B. Credit card number

    C. Published telephone number

    D. Driver's license number

12. Which of the following statements best describes the purpose of completing Department of Homeland Security/U.S. Citizenship and Immigration Services Form I-9 and providing supporting documentation?

    A. The purpose is to establish identity and employment authorization.

    B. The purpose is to determine tax identification and withholding.

    C. The purpose is to document educational achievements.

    D. The purpose is to verify criminal records.

13. The permissions and access rights a user is granted should match their role and responsibilities. Who is responsible for defining to whom access should be granted?

    A. The information user

    B. The information owner

    C. The information custodian

    D. The information author

14. Network administrators and help desk personnel often have elevated privileges. They are examples of which of the following roles?

    A. The information owners

    B. The information custodians

    C. The information authors

    D. The information sellers

15. Which of the following statements is *not* true of confidentiality agreements?

    A. Confidentiality/non-disclosure agreements are legal protection against unauthorized use of information.

    B. Confidentiality/non-disclosure agreements are generally considered a condition of work.

    C. Confidentiality/non-disclosure agreements are legally binding contracts.

    D. Confidentiality agreements should only be required of top-level executives.

16. Which of the following elements would you expect to find in an acceptable use agreement?

- **A.** Handling standards
- **B.** A lunch and break schedule
- **C.** A job description
- **D.** An evacuation plan

17. Which of the following statements best describes when acceptable use agreements should be reviewed, updated, and distributed?

- **A.** Acceptable use agreements should be reviewed, updated, and distributed only when there are organizational changes.
- **B.** Acceptable use agreements should be reviewed, updated, and distributed annually.
- **C.** Acceptable use agreements should be reviewed, updated, and distributed only during the merger and acquisition due diligence phase.
- **D.** Acceptable use agreements should be reviewed, updated, and distributed at the discretion of senior management.

18. Which of the following terms best describes the SETA acronym?

- **A.** Security Education Teaches Awareness
- **B.** Security Education Training Awareness
- **C.** Security Education Teaches Acceptance
- **D.** Security Education Training Acceptance

19. Posters are placed throughout the workplace reminding users to log off when leaving their workstations unattended. This is an example of which of the following programs?

- **A.** A security education program
- **B.** A security training program
- **C.** A security awareness program
- **D.** None of the above

20. A network engineer attends a one-week hands-on course on firewall configuration and maintenance. This is an example of which of the following programs?

- **A.** A security education program
- **B.** A security training program
- **C.** A security awareness program
- **D.** None of the above

21. The Board of Directors has a presentation on the latest trends in security management. This is an example of which of the following programs?

    A. A security education program

    B. A security training program

    C. A security awareness program

    D. None of the above

22. Companies have the legal right to perform which of the following activities?

    A. Monitor user Internet access from the workplace

    B. Place cameras in locker rooms where employees change clothes

    C. Conduct a search of an employee's home

    D. None of the above

23. Sanctions for policy violations should be included in which of the following documents?

    A. The employee handbook

    B. A confidentiality/non-disclosure agreement

    C. An acceptable use agreement

    D. All of the above

24. Studies often cite ____________ as the weakest link in information security.

    A. policies

    B. people

    C. technology

    D. regulations

25. Which of the following terms best describes the impact of security education?

    A. Long-term

    B. Short-term

    C. Intermediate

    D. Forever

26. Which of the following privacy regulations stipulates that schools must have written permission in order to release any information from a student's education record?

- **A.** Sarbanes-Oxley Act (SOX)
- **B.** HIPAA
- **C.** Gramm-Leach-Bliley Act (GLBA)
- **D.** FERPA

27. Which of the following regulations specifically stipulates that employees should be trained on password management?

- **A.** FERPA
- **B.** HIPAA
- **C.** DPPA
- **D.** FISMA

28. Best practices dictate that employment applications should *not* ask prospective employees to provide which of the following information?

- **A.** Last grade completed
- **B.** Current address
- **C.** Social security number
- **D.** Email address

29. After a new employee's retention period has expired, completed paper employment applications should be ___________.

- **A.** cross-cut shredded
- **B.** recycled
- **C.** put in the trash
- **D.** stored indefinitely

30. Intruders might find job posting information useful for which of the following attacks?

- **A.** A distributed denial of service attack (DDoS) attack
- **B.** A social engineering attack
- **C.** A man-in-the-middle attack
- **D.** An SQL injection attack

EXERCISES

EXERCISE 6.1: Analyzing Job Descriptions

1. Access an online job-posting service such as Monster.com.
2. Find two IT–related job postings.
3. Critique the postings. Do they reveal any information that a potential intruder could use in designing an attack such as the specific technology or software used by the organization, security controls, or organizational weaknesses?
4. Document your findings.

EXERCISE 6.2: Assessing Background Checks

1. Go online and locate one company that provides background checks.
2. What types of investigative services do they offer?
3. What information do you have to provide to them?
4. What is the promised delivery time?
5. Do they require permission from the target of the investigation?

EXERCISE 6.3: Learning What Your Social Media Says About You

1. What can a potential employer learn about you from your social media activities?
2. Look at the profile of a friend or acquaintance. What can a potential employer learn about him or her?

EXERCISE 6.4: Evaluating the Actions of Bad Employees

1. Locate a news article about a terminated or disgruntled employee who stole, exposed, compromised, or destroyed company information.
2. What could the company have done to prevent the damage?
3. In your opinion, what should be the consequences of the employee action?

EXERCISE 6.5: Evaluating Security Awareness Training

1. Either at your school or your place of work, locate and document at least one instance of a security awareness reminder.
2. In your opinion, is the reminder effective? Explain why or why not.
3. If you can’t locate an example of a security awareness reminder, compose a memo to senior management suggesting one.

PROJECTS

PROJECT 6.1: Evaluating the Hiring Process

1. Contact a local business and ask to speak with the Human Resources manager or hiring manager. Explain you are a college student working on a report and explain the information you need (see step 4) in order to complete the report. Request a 15-minute meeting.
2. At the meeting, ask the manager to explain the company's hiring process. Be sure to ask what (if any) background checks the company does and why. Also ask for a copy of a job application form. Don't forget to thank the person for his or her time.
3. After the meeting, review the application form. Does it include a statement authorizing the company to conduct background checks? Does it ask for any NPPI?
4. Write a report that covers the following:
   - Summary of meeting logistics (whom you meet with, where, and when)
   - Summary of hiring practices
   - Summary of any information shared with you that you would classify as protected or confidential (do not include specifics in your summary).

PROJECT 6.2: Evaluating an Acceptable Use Agreement

1. Locate a copy of your school or workplace acceptable use agreement (or equivalent document).
2. Write a critique of the agreement. Do you think that it includes enough detail? Does it explain why certain activities are prohibited or encouraged? Does it encourage users to be security conscious? Does it include sanction policy? Does it clearly explain the employee expectation of privacy? Can you tell when it was last updated? Are there any statements that are out of date?
3. Go back to Chapter 2, "Policy Elements and Style," and review the sections on using "plain language." Edit the agreement so that it conforms with plain language guidelines.

PROJECT 6.3: Evaluating Regulatory Training

1. Go online and locate an example of HIPAA security awareness training and GLBA security awareness training. (Note: You can use the actual training or an outline of topics.)
2. Document the similarities and differences.

Case Study: Designing a SETA Program

Anytown USA Bank prides itself on being very responsive to its customers. It offers a 24-hour staffed customer care center with a toll-free number. Over the past year, there has been a significant decline in calls and a corresponding increase in email service requests. As Information Security Officer (ISO), you are very concerned that customer information classified as "protected" is being sent via email or email attachments. You have requested a meeting with the Director of IT to explore "secure email" options since regular email is sent across the Internet in plain text. In the meantime, you want to make sure that employees understand the danger of using regular email.

1. Working with the training department, you are going to launch a security awareness campaign. The theme is "Email = Postcard." The message is that users should never write anything in an external email that they wouldn't write on a postcard.
   a. Create a security awareness campaign focused on this topic. Include in this plan specifics on how you intend to deliver the message.
   b. Create at least one piece of supporting collateral.
   c. Design a way to test the effectiveness of your message.
2. Before launching the campaign, you want to make sure you have the full support of the executive management.
   a. What type of "educational" program would you develop for management?
   b. What would the message be?
3. Outline the SETA program that will be needed to ensure the success of the "secure email" application.

References

"Employee Life Cycle," Search Financial Applications, accessed on 06/17/13, http://searchfinancialapplications.techtarget.com/definition/employee-life-cycle.

"Obtaining Security Clearance," Monster.com, accessed on 06/17/13, http://govcentral.monster.com/security-clearance-jobs/articles/413-how-to-obtain-a-security-clearance.

Regulations Cited

"26 U.S.C. 6103: Confidentiality and disclosure of returns and return information," accessed on 06/17/13, www.gpo.gov/fdsys/granule/USCODE-2011-title26/USCODE-2011-title26-subtitleF-chap61-subchapB-sec6103/content-detail.html.

"Americans with Disabilities Act (ADA)," official website of the United States Department of Justice, Civil Rights Division, accessed on 06/17/13, www.ada.gov/2010_regs.htm.

"Drivers Privacy Protection Act: DPPA," accessed on 06/17/13, http://uscode.house.gov/download/pls/18C123.txt.

"Fair Credit Reporting Act (FCRA). 15 U.S.C. 1681," accessed on 06/17/13, www.ftc.gov/os/statutes/031224fcra.pdf.

"Family Educational Rights and Privacy Act (FERPA)," official website of the U.S. Department of Education, accessed on 05/10/2013, www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

"Immigration Reform and Control Act of 1986 (IRCA)," official website of the U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services, accessed on 06/17/13, www.uscis.gov/.

"Public Law 108–159: Dec. 4, 2003 Fair and Accurate Credit Transactions Act of 2003," accessed on 06/17/13, www.gpo.gov/fdsys/pkg/PLAW-108publ159/.../PLAW-108publ159.pdf.

"Public Law No. 91-508: The Fair Credit Reporting Act," accessed on 06/17/13, www.ftc.gov/os/statutes/031224fcra.pdf.

"Sarbanes-Oxley Act—SoX," accessed on 06/17/13, http://uscode.house.gov/download/pls/15C98.txt www.sec.gov/about/laws/soa2002.pdf.

U.S. Department of Homeland Security and U.S. Citizenship and Immigration Services, Instructions for Employment Eligibility Verification.

U.S. Department of the Treasury and Internal Revenue Service, 2013 General Instructions for Forms W-2 and W-3.

Other Research

Beesley, Caron. "Conducting Employee Background Checks—Why Do It and What the Law Allows," SBA, accessed on 06/17/13, http://www.sba.gov/community/blogs/community-blogs/business-law-advisor/conducting-employee-background-checks-%E2%80%93-why-do.

"Houston Computer Administrator Sentenced to Two Years in Prison for Hacking Former Employer's Computer Network," Department of Justice, Office of Public Affairs, Press Release, July 15, 2009, accessed on 06/17/13, www.justice.gov/opa/pr/2009/July/09-crm-684.html.

"Jobs at Risk = Data at Risk," Ponemon Institute, accessed on 06/17/13, www.ponemon.org/data-security.

Messmer, Ellen. “More Than Half of Fired Employees Steal Data,” *CIO Magazine*, accessed on 06/17/13, www.cio.com/article/481883/More_Than_Half_of_Fired_Employees_Steal_Data.

“Rules for Conducting Employee Background Checks,” Jaburg-Wilk, accessed on 06/17/13, www.jaburgwilk.com/articles/employee-background-checks.aspx.

“Running Background Checks,” NOLO, accessed on 06/17/13, www.nolo.com/legal-encyclopedia/running-background-checks-job-applicants-29623.html.

Smith, Diane and Jacob Burg. “What Are the Limits of Employee Privacy?” American Bar Association, GP Solo, Volume 29, No. 6, accessed on 06/17/13, www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/what_are_limits_employee_privacy.html

“The General Electric (GE) Candidate Data Protection Standards,” accessed on 06/17/13, www.ge.com/careers/privacy.

Chapter 7

Physical and Environmental Security

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Define the concept of physical security and how it relates to information security.
- Evaluate the security requirements of facilities, offices, and equipment.
- Understand the environmental risks posed to physical structures, areas within those structures, and equipment.
- Enumerate the vulnerabilities related to reusing and disposing of equipment.
- Recognize the risks posed by the loss or theft of mobile devices and media.
- Develop policies designed to ensure the physical and environmental security of information, information systems, and information-processing and storage facilities.

In the beginning of the computer age, it was easy to protect the systems; they were locked away in a lab, weighed thousands of pounds, and only a select few were granted access. Today, computing devices are ubiquitous. We are tasked with protecting devices that range from massive cloud-based multiplex systems to tiny handheld devices. The explosion of both distributed and mobile computing means that computing devices can be located anywhere in the world and are subject to local law and custom. Possession requires that each individual user take responsibility for mobile device security.

Security professionals are often so focused on technical controls that they overlook the importance of physical controls. The simple reality is that physical access is the most direct path to malicious activity, including unauthorized access, theft, damage, and destruction. Protection mechanisms include controlling the physical security perimeter and physical entry, creating secure offices, rooms, and facilities, and implementing barriers to access, such as encryption, monitoring, and alerting. Section 11 of

ISO 27002:2013 encompasses both physical and environmental security. Environmental security refers to the workplace environment, which includes the design and construction of the facilities, how and where people move, where equipment is stored, how the equipment is secured, and protection from natural and man-made disasters.

In previous chapters, you learned that to properly protect organizational information we must first know where it is and how critical it is to the organization. Just as we shouldn't spend as much money or resources to protect noncritical information as we would to protect critical information, so it goes that we shouldn't spend the same amount to protect a broom closet as we should to protect information-processing facilities such as data centers, server rooms, or even offices containing client information.

Information security professionals rarely have the expertise to address this security domain on their own. It is critical to involve facilities and physical security personnel in strategic and tactical decisions, policies, and procedures. For example, the information security expert designs a server room with a double steel door, card-reading lock, and a camera outside the door. A facilities expert may question the construction of the walls, floor, vents, and ceilings, the capability of the HVAC and fire suppression systems, as well as the potential for a natural disaster, such as an earthquake, fire, or flood. A physical security expert may question the location, the topography, and even the traffic patterns of pedestrians, automobiles, and airplanes. Creating and maintaining physical and environmental security is a team effort.

In this chapter, we will be focusing on design, obstacles, monitoring, and response as they relate to secure areas, equipment security, and environmental controls. We will examine the security issues, related best practices, and of course physical and environmental security policies.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 11 of ISO 27002:2013 is dedicated to physical and environmental security, with the objective of maintaining a secure physical environment to prevent unauthorized access, damage, and interference to business premises. Special attention is paid to disposal and destruction.

Corresponding NIST guidance is provided in the following documents:

- SP 800-12: An Introduction to Computer Security—The NIST Handbook
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-88: Guidelines for Media Sanitization
- SP 800-100: Information Security Handbook: A Guide for Managers

Understanding the Secure Facility Layered Defense Model

The premise of a ***layered defense model*** is that if an intruder can bypass one layer of controls, the next layer of controls should provide additional deterrence or detection capabilities. Layered defense is both physical and psychological. The mere fact that an area *appears* to be secure is in itself a deterrent. Imagine the design of a medieval castle. The castle itself was built of stone. It was sited high on a hill within a walled property. There may have been a moat and an entry drawbridge. There were certainly lookouts and guards. In order for intruders to launch a successful attack, they had to overcome and penetrate each of these obstacles. The same concept is used in designing security buildings and areas.

FYI: Where the Internet Lives

In late 2012, *The New York Times* had a special series of articles detailing the environment and societal impact of mega data centers. Some of their major statistics included the following:

- There are more than three million data centers widely varying in size worldwide.
- Electricity used in global data centers likely accounted for between 1.1% and 1.5% in 2010.
- Worldwide data centers use about 30 billion watts of electricity, equivalent to the output of 30 nuclear power plants.
- Federal data centers grew from 432 in 1998 to 2,094 in 2010.

Why are these server farms mushrooming? According to IBM, 90% of the data in the world today has been created in the last two years alone.

To take a look at Google's data centers, go to www.google.com/about/datacenters.

You can view a photo gallery, take a "street view" tour, or even go on a guided video tour!

How Do We Secure the Site?

Depending on the size of the organization, information-processing facilities can range from a closet with one server to an entire complex of buildings with several thousand or even hundreds of thousands of computers. In addressing site physical security, we need to think of the most obvious risks, such as theft and other malicious activity, but we also must consider accidental damage and destruction related to natural disasters.

Location

The design of a secure site starts with the location. Location-based threats that need to be evaluated include political stability, susceptibility to terrorism, the crime rate, adjacent buildings, roadways, flight paths, utility stability, and vulnerability to natural disasters. Historical and predictive data can be used to establish both criminal and natural disaster chronology for a geographic area. The outcome will influence the type of security measures that an organization should implement. Best practices dictate that critical information-processing facilities be inconspicuous and unremarkable. They should not have signage relating to their purpose, nor should their outward appearance hint at what may be inside.

FYI: Crime Prevention Through Environmental Design (CPTED)

CPTED (pronounced *sep-ted*) has as its basic premise that the proper design and effective use of the physical environment can lead to a reduction in the incidence and fear of crime. CPTED is a psychological and sociological method of looking at security based upon three constructs:

- People protect territory they feel is their own, and people have a certain respect for the territory of others.
- Intruders do not want to be seen.
- Limiting access discourages intruders and/or marks them as intruders.

The International CPTED Association (ICA) is committed to creating safer environments and improving the quality of life through the use of CPTED principles and strategies. You can learn more about this design concept at www.cpted.net.

Perimeter Security

The three elements to security are obstacles that deter trivial attackers and delay serious ones, detection systems that make it more likely that the attack will be noticed, and a response capability to repel or catch attackers. Obstacles include physical elements such as berms, fences, gates, and bollards. Lighting is also a valuable deterrent. Entrances, exits, pathways, and parking lots should be illuminated. Fences should be at least eight feet in height, with a two-foot parameter of light used to illuminate along the top portion of the fence. The candlepower of the lighting must observe security standards. Detection systems include IP cameras, closed-circuit TV, alarms, motion sensors, and security guards. Response systems include locking gates and doors, on-site or remote security personnel notification, and direct communication with local, county, or state police.

In Practice

Physical Security Perimeter Policy

Synopsis: Securing the perimeter is the first line of defense against external physical attacks. Perimeter controls are required in order to prevent unauthorized access and damage to facilities.

Policy Statement:

- The company will establish physical security perimeters around business premises.
- An annual risk assessment of all existing business premises and information-processing facilities will be performed to determine the type and strength of the security perimeter that is appropriate and prudent.

- A risk assessment must be conducted on all new sites under consideration prior to building plans being finalized.
- The Office of Facilities Management in conjunction with the Office of Information Security will conduct the risk assessment.
- Risk assessment results and recommendations are to be submitted to the Chief Operating Officer (COO).
- The Office of Facilities Management is responsible for the implementation and maintenance of all physical security perimeter controls.

How Is Physical Access Controlled?

Our next area to consider is physical entry and exit controls. What does it take to get in and out? How is trouble detected and reported? Depending on the site and level of security required, a plethora of access controls are available, including cameras, security guards, mantraps, locks, barriers, metal detectors, biometric scanners, fire-resistant exterior walls that are solid and heavy, and unbreakable/shatterproof glass. The biggest challenge is authorized entry.

Authorizing Entry

How does a company identify authorized personnel such employees, contractors, vendors, and visitors? Of greatest concern becomes the fraudulent or forged credentials obtained through careful profiling or the carelessness of authenticated employees. One commonly used option is a badging system. Badges may also function as access cards. Visitors to secure areas should be credentialed and authorized. A number of visitor management systems facilitate ID scanning and verification, photo storage, credentialing, check-in and check-out, notifications, and monitoring. Visitors should be required to wear some kind of identification that can be evaluated from a distance. For instance, we might choose to have three different colored badges for visitors, which tell our employees what level of supervision should be expected, even if they view the person from across a 100-foot room. If a blue badge denotes close supervision, and you see someone wearing a blue badge without any supervision, you would know immediately to report the visitor or perhaps activate a silent alarm without having to confront or even come within close proximity of the individual.

In Practice

Physical Entry Controls Policy

Synopsis: Authorization and identification are required for entry to all non-public company locations.

Policy Statement:

- Access to all non-public company locations will be restricted to authorized persons only.
- The Office of Human Resources is responsible for providing access credentials to employees and contractors.

- The Office of Facilities Management is responsible for visitor identification, providing access credentials, and monitoring access. All visitor management activities will be documented.
- Employees and contractors are required to visibly display identification in all company locations.
- Visitors are required to display identification in all non-public company locations.
- Visitors are to be escorted at all times.
- All personnel must be trained to immediately report unescorted visitors.

Securing Offices, Rooms, and Facilities

In addition to securing building access, the organization needs to secure the workspaces within the building. Workspaces should be classified based on the level of protection required. The classification system should address personnel security, information systems security, and document security. The security controls must take into consideration workplace violence, intentional crime, and environmental hazards.

Secure design controls for spaces within a building include (but are not limited to) the following:

- Structural protection such as full height walls, fireproof ceilings, and restricted vent access
- Alarmed solid, fireproof, lockable, and observable doors
- Alarmed locking, unbreakable windows
- Monitored and recorded entry controls (keypad, biometric, card swipe)
- Monitored and recorded activity

In Practice

Workspace Classification

Synopsis: A classification system will be used to categorize workspaces. Classifications will be used to design and communicate baseline security controls.

Policy Statement:

- The company will use a four-tiered workspace classification schema consisting of secure, restricted, non-public, and public.
- The company will publish definitions for each classification.
- The criteria for each level will be maintained by and available from the Office of Facilities Management.
- All locations will be associated with one of the four data classifications. Classification assignment is the joint responsibility of the Office of Facilities Management and the Office of Information Security.

- Each classification must have documented security requirements.
- The COO must authorize exceptions.

Working in Secure Areas

It is not enough to just physically secure an area. Close attention must be paid to who is allowed to access the area and what they are allowed to do. Access control lists should be reviewed frequently. If the area is continually monitored, there should be guidelines specifying what is considered "suspicious" activity. If the area is videoed and not continually monitored, then there should be documented procedures regarding how often and by whom the video should be reviewed. Depending on the circumstances, it may be prudent to restrict cameras or recording devices, including smartphones, tablets, and USB drives, from being taken into the area.

In Practice

Working in Secure Areas Policy

Synopsis: Areas classified as "secure" will be continually monitored. Use of recording devices will be forbidden.

Policy Statement:

- All access to areas classified as "secure" will be continually monitored.
- All work in areas classified as "secure" will be recorded. The recordings will be maintained for a period of 36 months.
- Mobile data storage devices are prohibited and may not be allowed in areas classified as "secure" without the authorization of the system owner or Information Security Officer (ISO).
- Audio- and video-recording equipment is prohibited and may not be allowed in areas classified as "secure" without the authorization of the system owner or the Office of Information Security.
- This policy is in addition to workspace classification security protocols.

Ensuring Clear Desks and Clear Screens

Documents containing protected and confidential information are subject to intentional or accidental unauthorized disclosure unless secured from viewing by unauthorized personnel when not in use. The same holds true for computer screens. Companies have a responsibility to protect physical and digital information both during the workday and during non-business hours. All too often, organizations make it *easy* for unauthorized users to view information. Unauthorized access can be the result of viewing a document left unattended or in plain sight, removing (or reprinting) a document from a printer, copier, or fax machine, stealing digital media such as a DVD or USB drive, and even ***shoulder surfing***, which is the act of looking over someone's shoulder to see what is displayed on a monitor or device.

Protected or confidential documents should never be viewable by unauthorized personnel. When not in use, documents should be locked in file rooms, cabinets, or desk drawers. Copiers, scanners, and fax machines should be located in non-public areas and require use codes. Printers should be assigned to users with similar access rights and permissions and located close to the designated users. Users should be trained to retrieve printed documents immediately. Monitors and device screens should be situated to ensure privacy. Password-protected screen savers should be automated to engage automatically. Users should be trained to lock their screens when leaving devices unattended. Physical security expectations and requirements should be included in organizational acceptable use agreements.

FYI: CERT Case Files on Insider Theft

According to the CERT Insider Threat Blog entry from May 10, 2011, about 8% of crimes involving IT sabotage, theft of intellectual property, and fraud are related to physical access. Here are some of the cases they reviewed:

- For more than a year, a contract janitor stole customer account and personally identifiable information (PII) from hard-copy documents at a major U.S. bank. The janitor and two co-conspirators used this information to steal the identities of more than 250 people. They were able to open credit cards and then submit online change-of-address requests so the victims would not receive bank statements or other notifications of fraudulent activity. The insiders drained customers' accounts, and the loss to the organization exceeded $200,000.
- A communications director showed an expired ID badge to a security guard to gain unauthorized access to a data backup facility. Once inside, the director unplugged security cameras and stole backup tapes containing records for up to 80,000 employees.
- A contract security guard used a key to obtain physical access to a hospital's heating, ventilating, and air conditioning (HVAC) computer and another workstation. The guard used password-cracking software to obtain access and install malicious software on the machines. The incident could have affected temperature-sensitive patients, drugs, and supplies.
- An insider stole an organization's trade-secret drawings that were marked for destruction and sold them to a competing organization. The victim organization estimated its losses at $100 million. The competing organization that received the stolen documents was forced to declare bankruptcy after a lawsuit.

In Practice

Clear Desk and Clear Screen Policy

Synopsis: User controls are required to prevent the unauthorized viewing or taking of information.

Policy Statement:

- When left unattended during business hours, desks shall be clear of all documents classified as "protected" or "confidential."

- During non-business hours, all documents classified as "protected" or "confidential" will be stored in a secure location.
- While in use, device displays of any type must be situated to not allow unauthorized viewing.
- When left unattended during business hours, device displays should be cleared and locked to prevent viewing.
- Protected and confidential documents should only be printed to assigned printers. Print jobs should be retrieved immediately.
- Scanners, copiers, and fax machines must be locked when not in use and require user codes to operate.

Protecting Equipment

Now that we have defined how facilities and work areas will be secured, we must address the security of the equipment within these facilities. Traditionally, protection controls were limited to company-owned equipment. This is no longer the case. Increasingly, organizations are encouraging employees and contractors to "bring your own device" to work (referred to as BYOD). These devices may store, process, or transmit company information. In developing policies, we need to consider how best to protect both company- and employee-owned equipment from unauthorized access, theft, damage, and destruction.

No Power, No Processing?

No power, no processing—it's that simple. Long before computers took over the business world, organizations have been taking steps to ensure that power is available. Of course, it is now more important than ever. All information systems rely on clean, consistent, and abundant supplies of electrical power. Even portable devices that run on battery power require electricity for replenishment. Power is not free. Quite the contrary: Power can be very expensive, and excessive use has an environmental and geopolitical impact.

Energy Consumption

After lighting, computers and monitors have the highest energy consumption in office environments. As power consumption and costs rise, saving energy is becoming a significant issue. Using less energy depletes fuel at a lower rate, creates less pollution, and means less counterbalancing energy usage (for example, when the heat generated by a computer requires more air conditioning). Universities and Fortune 500 organizations have been leaders in the sustainable "green" computing movement. The goals of sustainable computing are to reduce the use of hazardous materials, maximize energy efficiency during the product's lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. One way to reduce consumption is to purchase Energy Star–certificated devices. ***Energy Star*** is a joint program of the U.S. Environmental Protection Agency and the U.S. Department of Energy to protect the environment through energy-efficient products and practices. There are strict guidelines that must be met, and only a limited percentage of products are accepted into the program. According to Google, one of the ways they have reduced data center energy consumption is to reduce cooling. Contrary to the misconception that data centers need to be kept chilly, most IT equipment can safely operate at 80°F or higher. Saving energy results in lower costs, less environmental impact, and a decreased dependence on global politics.

FYI: Reducing Energy Consumption

The following is an excerpt from Cornell University's *Facilities Services Sustainable Computing Guide*:

"A typical workstation consists of energy eating devices such as a computer, monitor, and any number of peripherals. It is possible to reduce daily consumption by up to 88%:

- "*Turn off peripherals when not in use.* Peripherals generally make up 10% of the total energy usage. Assuming an eight-hour workday, turning the peripherals off for the remaining 16 hours in the day would reduce the daily energy usage in the example by 6.7%.
- "*Turn off monitors when not in use.* Assuming that a typical user is only at their desk eight hours during the workday, this leaves 16 hours in which the monitor is not in use. Workstations configured to place the monitor into PowerSave mode during unused time could reduce daily energy usage by 24.5%.
- "*Turn off computers when not in use.* Powering down or placing a computer in standby mode will result in the largest drop in energy usage. Turning off the workstation for 16 of the 24 hours in a day would reduce the daily energy usage of that workstation by 62.3%.

"It is a myth that turning your computer off uses more energy than leaving it on. The surge of power used by a CPU to boot up is far less than the energy used by the unit when left on for over three minutes. One computer left on 24 hours a day dumps 1,500 pounds of CO_2 into the atmosphere annually. A tree absorbs between 3–15 pounds of CO_2 each year. That means that 100–500 trees would be needed to offset the yearly emissions of one computer left on all the time."

Power Protection

To function properly, our systems need consistent power delivered at the correct voltage level. Systems need to be protected from power loss, power degradation, and even from too much power, all of which can damage equipment. Common causes of voltage variation include lightning; damage to overhead lines from storms, trees, birds, or animals; vehicles striking poles or equipment; and load changes or equipment failure on the network. Heat waves can also contribute to power interruptions as the demand in electricity (that is, air conditioners) can sometimes exceed supply. The variation may be minor or significant.

Power flucuations are catagorized by changes in voltage and power loss:

- ***Power surges*** are prolonged increases in the voltage. A ***power spike*** is a momentary increase in voltage.
- ***Brownouts*** are prolonged periods of low voltage. A ***sag*** is a momentary low voltage.
- ***Blackouts*** are prolonged periods of power loss. A ***fault*** is a momentary loss of power.

Companies can install protective devices to help guard their premises and assets, such as installing surge protection equipment, line filters, isolation transformers, voltage regulators, power conditioners, uninterruptible power supplies (UPSs), and back-up power supplies. These power protection devices can condition the feed for consistency, provide continuous power for critical systems, and manage a controlled shutdown in the event of total loss of power.

In Practice

Power Consumption Policy

Synopsis: Power conditioning and redundancy protections must be in place to maintain the availability and performance of information systems and infrastructure. Power consumption should be minimized.

Policy Statement:

- The company is committed to sustainable computing and the minimization of power consumption.
- All computing devices purchased must be Energy Star (or equivalent) certified.
- All computing devices must be configured in power saver mode unless the setting degrades performance.
- A bi-annual assessment must be conducted by the Office of Facilities Management to determine the best method(s) to provide clean, reliable data center power.
- Data center equipment must be protected from damage caused by power fluctuations or interruptions.
- Data center power protection devices must be tested on a scheduled basis for functionality and load capacity. A log must be kept of all service and routine maintenance.
- Data center generators must be tested regularly according to manufacturer's instructions. A log must be kept of all service and routine maintenance.

How Dangerous Is Fire?

Imagine the impact of a data center fire—equipment and data irrevocably destroyed, internal communications damaged, and external connectivity severed. On July 3, 2009, multiple data centers at Seattle's Fisher Plaza were offline after a fire in an electrical vault, which left much of the complex without power and generator support. The payment portal Authorize.net was offline for hours, leaving thousands of merchants unable to process credit card payments through their websites. The downtime also affected Microsoft's Bing Travel service, Geocaching.com, domain registrar Dotster, and web hosting provider AdHost, along with dozens of other sites.

Fire protection is composed of three elements. Active and passive ***fire prevention controls*** are the first line of defense. Fire prevention controls include hazard assessments and inspections, adhering to building and construction codes, using flame-retardant materials, and proper handling and storage procedures for flammable/combustible materials. ***Fire detection*** is recognizing that there is a fire. Fire detection devices can be smoke activated, heat activated, or flame activated. ***Fire containment and suppression*** involve actually responding to the fire. Containment and suppression equipment is specific to fire classification. Data center environments are typically at risk to Class A, B, or C fires:

- **Class A**—Fire with combustible materials as its fuel source, such as wood, cloth, paper, rubber, and many plastics
- **Class B**—Fire in flammable liquids, oils, greases, tars, oil-base paints, lacquers, and flammable gases
- **Class C**—Fire that involves electrical equipment
- **Class D**—Combustibles that involve metals

Facilities must comply with standards to test fire-extinguishing methods annually to validate full functionality.

The best-case scenario is that data centers and other critical locations are protected by an automatic fire-fighting system that spans multiple classes. Like all other major investments, it's prudent to do a cost/benefit analysis before making a decision. In any emergency situation, human life always takes precedence. All personnel should know how to quickly and safely evacuate an area.

In Practice

Data Center and Communications Facilities Environmental Safeguards Policy

Synopsis: Data center and communications facilities must have controls designed to minimize the impact of power fluctuations, temperature, humidity, and fire.

Policy Statement:

- Smoking, eating, and drinking are not permitted in data center and communications facilities.
- Servers and communications equipment must be located in areas free from physical danger.

- Servers and communications must be protected by uninterruptable power supplies and back-up power sources.
- Appropriate fire detection, suppression, and fighting equipment must be installed and/or available in all data center and communications facilities.
- Appropriate climate control systems must be installed in all data center and communications facilities.
- Emergency lighting must engage automatically during power outages at all data center and communications facilities.
- The Office of Facilities Management is responsible for assessing the data center and communications facilities environmental requirements and providing the recommendations to the COO.
- The Office of Facilities Management is responsible for managing and maintaining the data center and communications facilities' climate-control, fire, and power systems.

What About Disposal?

What do servers, workstations, laptops, tablets, smartphones, firewalls, routers, copies, scanners, printers, memory cards, cameras, and flash drives have in common? They all store data that should be permanently removed before handing down, recycling, or discarding.

The data can be apparent, hidden, temporary, cached, browser based, or metadata:

- ***Apparent data files*** are files that authorized users can view and access.
- ***Hidden files*** are files that the operating system by design does not display.
- ***Temporary files*** are created to hold information temporarily while a file is being created.
- A ***web cache*** is the temporary storage of web documents, such as HTML pages, images, and downloads.
- A ***data cache*** is the temporary storage of data that has recently been read and, in some cases, adjacent data areas that are likely to be accessed next.
- ***Browser-based data*** includes the following items:
  - Browsing history, which is the list of sites visted
  - Download history, which is the list of files downloaded
  - Form history, which includes the items entered into web page forms
  - Search bar history, which includes items entered into the search engines
  - Cookies, which store information about websites visited, such as site preferences and login status
- ***Metadata*** is details about a file that describes or identifies it, such as title, author name, subject, and keywords that identify the document's topic or contents.

Removing Data from Drives

A common misconception is that deleting a file will permanently remove its data. ***Deleting*** (or trashing) a file removes the operating system pointer to the file. ***Formatting*** a disk erases the operating system address tables. In both cases, the files still reside on the hard drive, and system recovery software can be used to restore the data. To give you an idea of how easy it is to recover information from a formatted hard drive, simply Google the phrase "data recovery" and see what comes back to you. Utilities are available for less than $50 that are quite capable of recovering data from formatted drives. Even if a drive has been formatted and a new operating system installed, the data is recoverable.

NIST Special Publication 800-88 defines ***data destruction*** as "the result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive." There are two methods of permanently removing data from a drive—disk wiping (also known as scrubbing) and degaussing. The ***disk wiping*** process will overwrite the master boot record (MBR), partition table, and every sector of the hard drive with the numerals 0 and 1 several times. Then the drive is formatted. The more times the disk is overwritten and formatted, the more secure the disk wipe is. The government medium security standard (DoD 5220.22-M) specifies three iterations to completely overwrite a hard drive six times. Each iteration makes two write-passes over the entire drive; the first pass inscribes ones (1) over the drive surface and the second inscribes zeros (0) onto the surface. After the third iteration, a government-designated code of 246 is written across the drive, then it is verified by a final pass that uses a read-verify process. There are several commercially available applications that follow this standard. Disk wiping does not work reliability on solid-state drives; USB thumb drives, compact flash, and MMC/SD cards. ***Degaussing*** is the process wherein a magnetic object, such as a computer tape, hard disk drive, or CRT monitor, is exposed to a magnetic field of greater, fluctuating intensity. As applied to magnetic media, such as video, audio, computer tape, or hard drives, the movement of magnetic media through the degaussing field realigns the particles, resetting the magnetic field of the media to a near-zero state, in effect erasing all of the data previously written to the tape or hard drive. In many instances, degaussing resets the media to a like-new state so that it can be reused and recycled. In some instances, this simply wipes the media in preparation for safe and secure disposal. The National Security Agency (NSA) approves powerful degaussers that meet their specific standards and that in many cases utilize the latest technology for top-secret erasure levels.

Destroying Materials

The objective of physical ***destruction*** is to render the device and/or the media unreadable and unusable. Devices and media can be crushed, shredded, or, in the case of hard drives, drilled in several locations perpendicular to the platters and penetrating clear through from top to bottom.

Cross-cut shredding technology, which reduces material to fine, confetti-like pieces, can be used on all media, ranging from paper to hard drives.

It is common for organizations to outsource the destruction process. Companies that offer destruction services often have specialized equipment and are cognizant of environmental and regulatory requirements. The downside is that the organization is transferring responsibility for protecting information. The media may be transported to off-site locations. The data is being handled by non-employees over whom the originating organization has no control. Selecting a destruction service is serious business, and thorough due diligence is in order.

Both in-house and out-sourced destruction procedures should require that an unbroken pre-destruction ***chain of custody*** be maintained and documented and that an itemized post-destruction certificate of destruction be issued that serves as evidence of destruction in the event of a privacy violation, complaint, or audit.

FYI: Unscrubbed Hard Drives

In December 2010, a study commissioned by Britain's Information Commissioner's Office (IOC) found that 11% of second-hand hard drives sold online may contain residual personal information.

The IOC engaged an independent computer forensics company (NCC Group) to purchase and analyze approximately 200 hard disk drives, 20 memory sticks, and ten mobile telephones. These were bought from a variety of sources, with most coming from online auction sites. NCC first examined the drives using no additional software to see what information was immediately evident. The drives were then studied using forensic tools freely available on the Internet. This was carried out to replicate the attempts that more knowledgeable individuals may make to try and recover data for improper usage.

Here are the findings:

- Negligible personal data was found on the memory sticks and mobile telephones.
- In the case of hard drives:
  - Thirty-eight percent of the devices had been wiped of data.
  - Fourteen percent were damaged/unreadable.
  - Thirty-seven percent contained non-personal data.
  - Eleven percent contained personal data, including copies of passports, birth certificates, and drivers licenses, bank statements, tax information, and medical records.

In total, some 34,000 files were found containing personal or corporate data. The most significant finding was that the drives were from computers that were either personally or corporately owned, and in some cases, the user was not authorized to store the data.

In Practice

Secure Disposal Policy

Synopsis: All media must be disposed of in a secure and environmentally sound manner.

Policy Statement:

- The Office of Facilities Management and the Office of Information Security are jointly responsible for determining the disposal standards for each classification of information.
- Devices or media containing “protected” or “confidential” information must not be sent off-site for repair and/or maintenance.
- The standards for the highest classification must be adhered to when the device or media contains multiple types of data.
- A chain of custody must be maintained for the destruction of “protected” and “confidential” information.
- A certificate of destruction is required for third-party destruction of devices or media that contains “protected” and “confidential” information.
- Disposal of media and equipment will be done in accordance with all applicable state and federal environmental disposal laws and regulations.

Stop, Thief!

According to the Federal Bureau of Investigation (FBI), on average, a laptop is stolen every 53 seconds and one in ten individuals will have their laptop stolen at some point. The recovery statistics of stolen laptops is even worse, with only 3% ever being recovered. This means 97% of laptops stolen will never be returned to their rightful owners. A 2010 independent study conducted by the Ponemon Institute reported that 43% of laptops were lost or stolen off-site (working from a home office or hotel room), 33% lost or stolen in travel or transit, and 12% lost or stolen in the workplace. The statistics for mobile phones and tablets is even worse. According to an American Public Media May 2013 Marketplace Morning report, cell phone theft accounts for 30% to 40% of all crime in major cities—40% in New York and Washington, D.C., and 50% in San Francisco.

The cost of lost and stolen devices is significant. The most obvious loss is the device itself. The cost of the device pales in comparison to the cost of detection, investigation, notification, after-the-fact response, and economic impact of lost customer trust and confidence, especially if the device contained legally protected information. The Ponemon Institute “2013 Cost of Data Breach Study: Global Analysis” calculated the average business cost of a breach in the United States to be $188 per record across all industries, $215 per record for financial institutions, and $233 per record for healthcare organizations.

Consider this scenario: A laptop valued at $1,500 is stolen. A file on the laptop has information about 2,000 patients. Using the Ponemon conclusion of $215 per record, the cost of the compromise would be $430,000! That cost doesn’t include potential litigation or fines.

FYI: Week of June 24, 2013—26,825 Personal Records Reported Compromised

Date Reported	Organization	Description	# of Records	Info Exposed	Details
6/24/13	Kings County Sheriff's Office, Seattle, WA	Stolen laptop	2,300	Case files, including social security and driver's license numbers, about thousands of crime victims, suspects, witnesses, and even police officers.	Laptop was stolen the previous March from the backseat of a detective's undercover pickup truck.
6/24/13	LifeLabs Medical Laboratory Services, Vancouver, B.C.	Stolen hard drive	16,100	Names, addresses, dates of birth, and gender and medical information.	Hard drive was stolen out of a laptop sent for repair.
6/30/13	Wedgewood Legacy Medical, Lincoln, NE	Lost thumb drive	2,125	Patients' full names, birth dates, home addresses, phone numbers and, in some cases, names of family members.	A physician was wearing the thumb drive on a lanyard around his neck and it was said to have slipped off.
6/30/13	University of South Carolina, Columbia, SC	Stolen laptop	6,300	Names, email addresses, and social security numbers.	A laptop was stolen from a locked room in the university's physics and astronomy department that contained the student information.

In Practice

Mobile Device and Media Security

Synopsis: Safeguards must be implemented to protect information stored on mobile devices and media.

Policy Statement:

- All company-owned and employee-owned mobile devices and media that store or have the potential to store information classified as “protected” or “confidential” must be encrypted.
- Whenever feasible, an antitheft technology solution must be deployed that enables remote locate, remote lock, and remote delete/wipe functionality.
- Loss or theft of a mobile device or media must be reported immediately to the Office of Information Security.

FYI: Small Business Note

Two physical security issues are specific to small business and/or remote offices: location and person identification. A majority of small business and remote offices are located in multitenant buildings, where occupants do not have input into or control of perimeter security measures. In this case, the organization must treat their entry doors as the perimeter and install commensurate detective and preventative controls. Often, tenants are required to provide access mechanisms (for example, keys, codes) to building personnel, such as maintenance and security. Unique entry codes should be assigned to third-party personnel so that entry can be audited. Rarely are employee identification badges used in a small office. This makes it all the more important that visitors be clearly identified. Because there is little distinction between public and private spaces, visitors should be escorted whenever they need to go on the premises.

Summary

The objective of physical and environmental security is to prevent unauthorized access, damage, and interference to business premises and equipment. In this chapter, with a focus on the physical environment, we discussed the three elements to security—obstacles that deter trivial attackers and delay serious ones, detection systems that make it more likely that the attack will be noticed, and a response capability to repel or catch attackers. We began at the security perimeter, worked our way gradually inward to the data center, and then back out to mobile devices. Starting at the perimeter, we saw the importance of having a layered defense model as well as incorporating CPTED (crime prevention through environmental design) concepts. Moving inside the building, we looked at entry controls and the challenge of authorized access and identification. We acknowledged that not all access is equal. Workspaces and areas need to be classified so that levels of access can be determined and appropriate controls implemented. Equipment needs to be protected from damage, including natural disasters, voltage variations (such as surges, brownouts, and blackouts), fire, and theft. Purchasing Energy Star–certified equipment and proactively reducing energy consumption supports the long-term security principle of availability.

We explored the often-overlooked risks of device and media disposal and how important it is to permanently remove data before handing down, recycling, or discarding devices. Even the most innocuous devices or media may contain business or personal data in metadata, hidden or temporary files, web or data caches, or the browser history. Deleting files or formatting drives is not sufficient. DoD-approved disk-wiping software or a degaussing process can be used to permanently remove data. The most secure method of disposal is destruction, which renders the device and/or the media unreadable and unusable.

Mobile devices that store, process, or transmit company data are the newest challenge to physical security. These devices travel the world and in some cases are not even company owned. Threats range the gamut from nosy friends and colleagues to targeted theft. The detection, investigation, notification, and after-the-fact response cost of a lost or stolen mobile device is astronomical. The economic impact of lost customer trust and confidence is long lasting. Encryption and antitheft technology solutions that enable remote locate, remote lock, and remote delete/wipe functionality must be added to the protection arsenal.

Physical and environmental security policies include perimeter security, entry controls, workspace classification, working in secure areas, clean desk and clean screen, power consumption, data center and communications facilities environmental safeguards, secure disposal, and mobile device and media security.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following groups should be assigned responsibility for physical and environmental security?

   A. Facilities management

   B. Information security management

   C. Building security

   D. A team of experts including facilities, information security, and building security

2. Physical and environmental security control decisions should be driven by a(n) ___________.

   A. educated guess

   B. industry survey

   C. risk assessment

   D. risk management

3. Which of the following terms best describes CPTED?

   A. Crime prevention through environmental design

   B. Crime prevention through environmental designation

   C. Criminal prevention through energy distribution

   D. Criminal prosecution through environmental design

4. Which of the following is a CPTED strategy?

   A. Natural surveillance.

   B. Territorial reinforcement.

   C. Natural access control.

   D. All of the above are CPTED strategies.

5. Which of the following models is known as the construct that if an intruder can bypass one layer of controls, the next layer of controls should provide additional deterrence or detection capabilities?

   A. Layered defense model

   B. Perimeter defense model

   C. Physical defense model

   D. Security defense model

6. Which of the following is a location-based threat?

   A. Flight path

   B. Volcano

   C. Political stability

   D. All of the above

7. Best practices dictate that data centers should be ______________.

   A. well marked

   B. located in urban areas

   C. inconspicuous and unremarkable

   D. built on one level

8. Which of the following would be considered a “detection” control?

   A. Lighting

   B. Berms

   C. Motion sensors

   D. Bollards

9. Badging or an equivalent system at a secure facility should be used to identify ____________.

   A. everyone who enters the building

   B. employees

   C. vendors

   D. visitors

10. Which of the following statements best describes the concept of shoulder surfing?

    A. Shoulder surfing is the use of a keylogger to capture data entry.

    B. Shoulder surfing is the act of looking over someone’s shoulder to see what is on a computer screen.

    C. Shoulder surfing is the act of positioning one’s shoulders to prevent fatigue.

    D. None of the above.

11. The term BYOD is used to refer to devices owned by ____________.

12. Which of the following statements is *not* true about reducing power consumption?

    A. Reducing power consumption saves energy.

    B. Reducing power consumption saves money.

    C. Reducing power consumption creates less pollution.

    D. Reducing power consumption increases CO2 emissions.

13. The United States government Energy Star certification indicates which of the following?

    A. The product is a good value.

    B. The product was made in the United States.

    C. The product has met energy efficiency standards.

    D. The product is used by the government.

14. Which of the following actions contribute to reducing daily power consumption?

    A. Turning off computers when not in use

    B. Turning off monitors when not in use

    C. Turning off printers when not in use

    D. All of the above

15. Which of the following terms best describes a prolonged increase in voltage?

    A. Power spike

    B. Power surge

    C. Power hit

    D. Power fault

16. Common causes of voltage variations include _______________.

    A. lightning, storm damage, and electric demand

    B. using a power conditioner

    C. turning on and off computers

    D. using an uninterruptable power supply

17. Adhering to building and construction codes, using flame-retardant materials, and properly grounding equipment are examples of which of the following controls?

    A. Fire detection controls

    B. Fire containment controls

    C. Fire prevention controls

    D. Fire suppression controls

18. A Class C fire indicates the presence of which of the following items?

    A. Electrical equipment
    B. Flammable liquids
    C. Combustible materials
    D. Fire extinguishers

19. Classified data can reside on which of the following items?

    A. Smartphones
    B. Cameras
    C. Scanners
    D. All of the above

20. Which of the following data types includes details about a file or document?

    A. Apparent data
    B. Hidden data
    C. Metadata
    D. Cache data

21. URL history, search history, form history, and download history are stored by the device ___________.

    A. operating system
    B. browser
    C. BIOS
    D. None of the above

22. Which of the following statements about formatting a drive is not true?

    A. Formatting a drive creates a bootable partition.
    B. Formatting a drive overwrites data.
    C. Formatting a drive fixes bad sectors.
    D. Formatting a drive permanently deletes files.

23. Disk wiping works reliably on which of the following media?

    A. USB thumb drives
    B. Conventional hard drives
    C. SD cards
    D. Solid-state hard drives

24. The United States Department of Defense (DoD) medium security disk-wiping standard specifies which of the following actions?

    A. Three iterations to completely overwrite a hard drive six times

    B. Three iterations to completely overwrite a hard drive six times, plus 246 written across the drive

    C. Three iterations to completely overwrite a hard drive six times, plus 246 written across the drive, plus a read-verify process

    D. Three iterations to completely overwrite a hard drive six times, plus 246 written across the drive, plus a magnetic swipe

25. Which of the following terms best describes the process of using a realigning and resetting particle to erase data?

    A. Deleting

    B. Degaussing

    C. Destroying

    D. Debunking

26. Which of the following terms best describes the shredding technique that reduces material to fine, confetti-like pieces?

    A. Cross-cut

    B. Strip-cut

    C. Security-cut

    D. Camel-cut

27. A certificate of destruction is evidence that __________________.

    A. the media has be destroyed by a third party

    B. the media has been destroyed internally

    C. the media has been destroyed by its owner

    D. the media has been destroyed

28. Which of the following amounts represents the average per-record cost of a data breach in the United States?

    A. $1

    B. $18

    C. $188

    D. $1,188

29. Which of the following controls includes remote lock, remote wipe, and remote location?

    A. Work-at-home controls

    B. Mobile device antitheft controls

    C. GPS controls

    D. Find-my-car controls

30. In an environmental disaster, priority should be given to _______________.

    A. protecting human life

    B. saving key documents

    C. data center continuity

    D. first responder safety

EXERCISES

EXERCISE 7.1: Researching Data Destruction Services

1. Research companies in your area that offer data destruction services.
2. Document the services they offer.
3. Make a list of questions you would ask them if you were tasked with selecting a vendor for data destruction services.

EXERCISE 7.2: Assessing Data Center Visibility

1. Locate the data center at your school or workplace.
2. Is the facility or area marked with signage? How easy was it to find? What controls are in place to prevent unauthorized access? Document your findings.

EXERCISE 7.3: Reviewing Fire Containment

1. Find at least three on-campus fire extinguishers (do not touch them). Document their location, what class fire they can be used for, and when they were last inspected.
2. Find at least one fire extinguisher (do not touch it) in your dorm, off-campus apartment, or home. Document the location, what class fire it can be used for, and when it was last inspected.

EXERCISE 7.4: Assessing Identification Types

1. Document what type of identification is issued to students, faculty, staff, and visitors at your school. If possible, include pictures of these types of documentation.
2. Describe the process for obtaining student identification.
3. Describe the procedure for reporting lost or stolen identification.

EXERCISE 7.5: Finding Data

1. Access a public computer in either the library, computer lab, or classroom.
2. Find examples of files or data that other users have left behind. The files can be apparent, temporary, browser based, cached, or document metadata. Document your findings.
3. What should you do if you discover "personal" information?

PROJECTS

PROJECT 7.1: Assessing Physical and Environmental Security Assessment

1. You are going to conduct a physical assessment of a computing device you own. This could be a desktop computer, a laptop, a tablet, or a smartphone. Use the following table as a template to document your findings. You can add additional fields.

Device Description: Laptop Computer

							Safeguard		
Threats/ Danger	Impact	Safeguard 1	Safeguard 2	Safeguard 3	Assessment	Recommendation	Initial Cost	Annual Cost	Cost/ Benefit Analysis
Lost or forgotten	Need laptop for school-work	Pink case	Labeled with owner's contact info	--	Inadequate	Install remote find software	$20.00	$20.00	$20 per year vs. the cost of replacing the laptop

2. Determine the physical and environmental dangers (threats); for example, losing or forgetting your laptop at school. Document your findings.
3. For each danger (threat), identify the controls that you have implemented; for example, your case is pink (recognizable) and the case and laptop are labeled with your contact information. It is expected that not all threats will have corresponding safeguards. Document your findings.
4. For threats that do not have a corresponding safeguard or ones for which you feel the current safeguards are inadequate, research the options you have for mitigating the danger. Based on your research, make recommendations. Your recommendation should include initial and ongoing costs. Compare the costs of the safeguard to the cost impact of the danger. Document your findings.

PROJECT 7.2: Assessing Data Center Design

1. You have been tasked with recommending environmental and physical controls for a *new* data center to be built at your school. You are expected to present a report to the Chief Information Officer. The first part of your report should be a synopsis of the importance of data center physical and environmental security.

2. The second part of your report should address three areas: location, perimeter security, and power.

   a. Location recommendations should include where the data center should be built and a description of the security of the surrounding area (for example, location-based threats include political stability, susceptibility to terrorism, the crime rate, adjacent buildings, roadways, pedestrian traffic, flight paths, utility stability, and vulnerability to natural disasters).

   b. Access control recommendations should address who will be allowed in the building and how they will be identified and monitored.

   c. Power recommendations should take into account power consumption as well as normal and emergency operating conditions

PROJECT 7.3: Securing the Perimeter

1. The security perimeter is a barrier of protection from theft, malicious activity, accidental damage, and natural disaster. Almost all buildings have multiple perimeter controls. We have become so accustomed to perimeter controls that they often go unnoticed (that is, security guards). Begin this project with developing a comprehensive list of perimeter controls.

2. Conduct a site survey by walking around your city or town. You are looking for perimeter controls. Include in your survey results the address of the building, a summary of building occupants, type(s) of perimeter controls, and your opinion as to the effectiveness of the controls. In order to make your survey valid, you must include at least ten properties.

3. Choose one property to focus on. Taking into consideration the location, the depth security required by the occupants, and the geography, comment in detail on the perimeter controls. Based on your analysis, recommend additional physical controls to enhance perimeter security.

Case Study

Physical Access Social Engineering

In your role of ISO at Anywhere USA University Teaching Hospital, you commissioned an independent security consultancy to test the hospital's physical security controls using social engineering impersonation techniques. At the end of the first day of testing, the tester submitted a preliminary report.

Physical Access to Facilities

Dressed in blue scrubs, wearing a stethoscope, and carrying a clipboard, the tester was able to access the lab, the operating room, and the maternity ward. In one case, another staff member buzzed him in. In the two other cases, the tester walked in with other people.

Physical Access to the Network

Dressed in a suit, the tester was able to walk into a conference room and plug his laptop into a live data jack. Once connected, he was able to access the hospital's network.

Physical Access to a Computer

Wearing a polo shirt with a company name, the tester was able to sit down at an unoccupied office cubicle and remove a hard disk from a workstation. When questioned, he answered that he had been hired by John Smith, IT Manager to repair the computer.

Physical Access to Patient Files

Wearing a lab coat, the tester was able to walk up to a printer in the nursing station and remove recently printed documents.

Based on these findings, you request that the consultancy suspend the testing. Your immediate response is to call a meeting to review the preliminary report.

1. Determine who should be invited to the meeting.
2. Compose a meeting invitation explaining the objective of the meeting.
3. Prepare an agenda for the meeting.
4. Identify what you see as the most immediate issues to be remediated.

References

Regulations Cited

DoD 5220.22-M: National Industrial Security Program Operating Manual, February 28, 2006, revised March 28, 2013.

Other References

"About Energy Star," Energy Star, accessed on 06/2013, www.energystar.gov.

"Computer Energy Usage Facts," Cornell University, accessed on 06/28/2013, http://computing.fs.cornell.edu/Sustainable/fsit_facts.cfm.

Bray, Megan, "Review of Computer Energy Consumption and Potential Savings," December 2006, accessed on 06/2013, www.dssw.co.uk/research/computer_energy_consumption.html.

"Efficiency: How we do it," Google, accessed on 6/28/2013, www.google.com/about/datacenters/efficiency/internal/index.html#temperature.

"Facilities Services Sustainable Computing Guide," Cornell University, accessed on 06/2013, http://computing.fs.cornell.edu/Sustainable/FSSustainableComputingGuide.pdf.

"Foundations Recovery Network notifying patients after a laptop with PHI was stolen from an employee's car," PHIprivacy.net, June 24, 2013, accessed on 06/2013, www.phiprivacy.net/?p=12980.

Glanz, James, "The Cloud Factories: Data Barns in a Farm Town, Gobbling Power and Flexing Muscle," *The New York Times*, September 23, 2012, accessed on 06/2013, www.nytimes.com/2012/09/24/technology/data-centers-in-rural-washington-state-gobble-power.html?pagewanted=all&_r=2&.

"Tripplite Glossary," accessed on 06/2013, www.tripplite.com/support/glossary.cfm.

"Google Data Centers," Google.com, accessed on 06/2013, www.google.com/about/datacenters/.

"Insider Threat and Physical Security of Organizations," CERT Insider Threat Center, May 20, 2011, accessed on 06/2013, www.cert.org/blogs/insider_threat/2011/05/insider_threat_and_physical_security_of_organizations.html.

Jeffery, C. Ray, *Crime Prevention Through Environmental Design, Second Edition*, Beverly Hills: Sage Publications, 1977.

"Laptop Theft Recovery," Winthrop University, accessed on 06/2013, www.winthrop.edu/police.

"Latest Incidents," DataLossDB, accessed on 06/2013, http://datalossdb.org/.

Marshall-Genzar, Nancy, "Cell phone theft is on the rise, but the industry isn't helping much (Infographic)," Marketplace Morning Report for Tuesday May 14, 2013, accessed on 06/2013, www.marketplace.org/topics/business/cell-phone-theft-rise-industry-isnt-helping-much-infographic.

Miller, Rich "Major Outage at Seattle Data Center," Data Center Knowledge, July 3, 2009, accessed on 06/2013, www.datacenterknowledge.com/archives/2009/07/03/major-outage-at-seattle-data-center.

Ponemon Institute, "The Billion Dollar Lost Laptop Problem: Benchmark Study of U.S. Organization." October 31, 2010.

Ponemon Institute, "2013 Cost of Data Breach Study." May, 2013.

"Stolen Laptop May Have Compromised Students Personal Info," ABC Columbia, June 27, 2013, accessed on 06/2013, www.abccolumbia.com/news/local/Stolen-Laptop-May-Have-Compromised-Students-Personal-Info-213435101.html.

"Unscrubbed Hard Drives Report," Information Commissioner's Office, April 25, 2012, accessed on 06/2013, http://www.ico.org.uk/news/latest_news/2012/~/media/documents/library/Data_Protection/Research_and_reports/unscrubbed_hard_drives_report.pdf.

Vanhorn, Chris, “Cornell University Facilities Services Computing Energy Conservation Recommendations,” September 8, 2005, accessed on 06/28/2013, http://computing.fs.cornell.edu/Sustainable/ComputingEnergyConservation.pdf.

Vedder, Tracy, “Detective’s stolen laptop puts thousands at risk of identity theft,” KOMONEWS, June 24, 2013, accessed on 06/2013, www.komonews.com/news/local/Stolen-sheriffs-office-laptop-puts-thousand-at-risk-of-identity-theft-212860341.html.

“Voltage Variations,” United Energy and Multinet Gas, accessed on 6/28/2013,
www.unitedenergy.com.au/customers/your-electricity/electricity-outages/voltage-variations.aspx.

“Your Guide To Degaussers,” Degausser.com, accessed on 06/2013, http://degausser.com/.

Chapter 8

Communications and Operations Security

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Author useful standard operating procedures
- Implement change control processes
- Understand the importance of patch management
- Protect information systems against malware
- Consider data backup and replication strategies
- Recognize the security requirements of email and email systems
- Appreciate the value of log data and analysis
- Evaluate service provider relationships
- Write policies and procedures to support operational and communications security

Section 11 of ISO 27002:2013, "Communications Security," and Section 15 of ISO 27002:2013, "Operations Security," focus on information technology (IT) and security functions, including standard operating procedures, change management, malware protection, data replication, secure messaging, and activity monitoring. These functions are primarily carried out by IT and information security data custodians such as network administrations and security engineers. Many companies outsource some aspect of their operations. Section 15 of ISO 27002:2013, "Supplier Relationships," focuses on service delivery and third-party security requirements.

The Security Education, Training, and Awareness model (SETA) introduced in Chapter 6, "Human Resources Security," is particularly appropriate for this domain. Data owners need to be educated on operational risk so they can make informed decisions. Data custodians should participate in training that focuses on operational security threats so that they understand the reason for implementing safeguards. Users should be surrounded by a security awareness program that fosters everyday best practices. Taken together, SETA will enhance policy acceptance and stewardship. Throughout the chapter, we cover policies, processes, and procedures recommended to create and maintain a secure operational environment.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 12 of ISO 27002:2013, "Operations Security," focuses on data center operations, integrity of operations, vulnerability management, protection against data loss, and evidence-based logging. Section 13 of ISO 27002:2013, "Communications Security," focuses on protection of information in transit. Section 15 of ISO 27002:2013, "Supplier Relationships," focuses on service delivery and third-party security requirements.

Corresponding NIST guidance is provided in the following documents:

- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations
- SP 800-100: Information Security Handbook: A Guide for Managers
- SP 800-40: Creating a Patch and Vulnerability Management Program
- SP 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- SP 800-45: Guidelines on Electronic Mail Security
- SP 800-92: Guide to Computer Security Log Management
- SP 800-42: Guideline on Network Security Testing

Standard Operating Procedures (SOPs)

Standard operating procedures (SOPs) are detailed explanations of how to perform a task. The objective of an SOP is to provide standardized direction, improve communication, reduce training time, and improve work consistency. An alternate name for SOPs is *standard operating protocols*. An effective SOP communicates who will perform the task, what materials are necessary, where the task will take place, when the task will be performed, and how the person will execute the task.

Why Document SOPs?

The very process of creating SOPs requires us to evaluate what is being done, why it is being done that way, and perhaps how we could do it better. SOPs should be written by individuals knowledgeable with the activity and the organization's internal structure. Once written, the details in an SOP standardize the target process and provide sufficient information that someone with limited experience with or knowledge of the procedure but with a basic understanding can successfully perform the procedure unsupervised. Well-written SOPs reduce organizational dependence on individual and institutional knowledge.

It is not uncommon for an employee to become so important that losing that individual would be a huge blow to the company. Imagine that this person is the only one performing a critical task, no one has been cross-trained, and no documentation as to how he performs this task exists. The employee suddenly becoming unavailable could seriously injure the organization. Having proper documentation of operating procedures is not a luxury: It is a business requirement.

Authorizing SOP Documentation

Once a procedure has been documented, it should be reviewed, verified, and authorized before being published. The reviewer analyzes the document for clarity and readability. The verifier tests the procedure to make sure it is correct and not missing any steps. The process owner is responsible for authorization, publication, and distribution. Post-publication changes to the procedures must be authorized by the process owner.

Protecting SOP Documentation

Access and version controls should be put in place to protect the integrity of the document from both unintentional error and malicious insiders. Imagine a case where a disgruntled employee gets hold of a business-critical procedure document and changes key information. If the tampering is not discovered, it could lead to a disastrous situation for the company. The same holds true for revisions. If multiple revisions of the same procedure exist, there is a good chance someone is going to be using the wrong version.

Developing SOPs

SOPs should be understandable to everyone who uses them. SOPs should be written in a concise, step-by-step, ***plain language*** format. If not well written, SOPs are of limited value. It is best to use short, direct sentences so that the reader can quickly understand and memorize the steps in the procedure. Information should be conveyed clearly and explicitly to remove any doubt as to what is required. The steps must be in logical order. Any exceptions must be noted and explained. Warnings must stand out.

The four common SOP formats are simple step, hierarchical, flowchart, and graphic. As shown in Table 8.1, two factors determine what type of SOP to use: how many decisions the user will need to make and how many steps are in the procedure. Routine procedures that are short and require few decisions can be written using the simple step format. Long procedures consisting of more than ten steps, with few decisions, should be written in a hierarchical format or in a graphic format. Procedures that require many decisions should be written in the form of a flowchart. It is important to choose the correct format. The best-written SOPs will fail if they cannot be followed.

TABLE 8.1 SOP Methods

Many Decisions?	More Than Ten Steps?	Recommended SOP Format
No	No	Simple Step
No	Yes	Hierarchical or Graphic
Yes	No	Flowchart
Yes	Yes	Flowchart

As illustrated in Table 8.2, the simple step format uses sequential steps. Generally, these rote procedures do not require any decision-making and do not have any sub-steps. The simple step format should be limited to ten steps.

TABLE 8.2 Simple Step Format

Procedure	Completed
Note: These procedures are to be completed by the night operator by 6:00 a.m., Monday–Friday. Please initial each completed step.	
1. Remove backup tape from tape drive.	
2. Label with the date.	
3. Place tape in tape case and lock.	
4. Call ABC delivery at 888-555-1212.	
5. Tell ABC that the delivery is ready to be picked up.	
6. When ABC arrives, require driver to present identification.	
7. Note in pickup log the driver's name.	
8. Have the driver sign and date the log.	

As illustrated in the New User Account Creation Procedure example, shown in Table 8.3, the hierarchical format is used for tasks that require more detail or exactness. The hierarchical format allows the use of easy-to-read steps for experienced users while including sub-steps that are more detailed as well. Experienced users may only refer to the sub-steps when they need to, whereas beginners will use the detailed sub-steps to help them learn the procedure.

TABLE 8.3 Hierarchical Format

New User Account Creation Procedure	
Note: You must have the HR New User Authorization Form before starting this process.	
Procedures	**Detail**
Launch Active Directory Users and Computers (ADUC).	a. Click on the TS icon located on the administrative desktop. b. Provide your login credentials. c. Click the ADUC icon.
Create a new user.	a. Right-click the Users OU folder. b. Choose New User.
Enter the required user information.	a. Enter user first, last, and full name. b. Enter user login name and click Next. c. Enter user's temporary password. d. Choose User Must Change Password at Next Login and click Next.
Create an Exchange mailbox.	a. Make sure Create an Exchange Mailbox is checked. b. Accept the defaults and click Next.
Verify account information.	a. Confirm that all information on the summary screen is correct. b. Choose Finish.
Complete demographic profile.	a. Double-click the user name. b. Complete the information on the General, Address, Telephone, and Organization tabs. (Note: Info should be on the HR request sheet.)
Add users to groups.	a. Choose the Member Of tab. b. Add groups as listed on the HR request sheet. c. Click OK when completed.
Set remote control permissions.	a. Click the Remote Control tab. b. Make sure the Enable Remote Control and Require User's Permission boxes are checked. c. Level of control should be set to Interact with the Session.
Advise HR regarding account creation.	a. Sign and date the HR request form. b. Send it to HR via interoffice mail.

Pictures truly are worth a thousand words. The graphic format, shown in Figure 8.1, can use photographs, icons, illustrations, or screenshots to illustrate the procedure. This format is often used for configuration tasks, especially if various literacy levels or language barriers are involved.

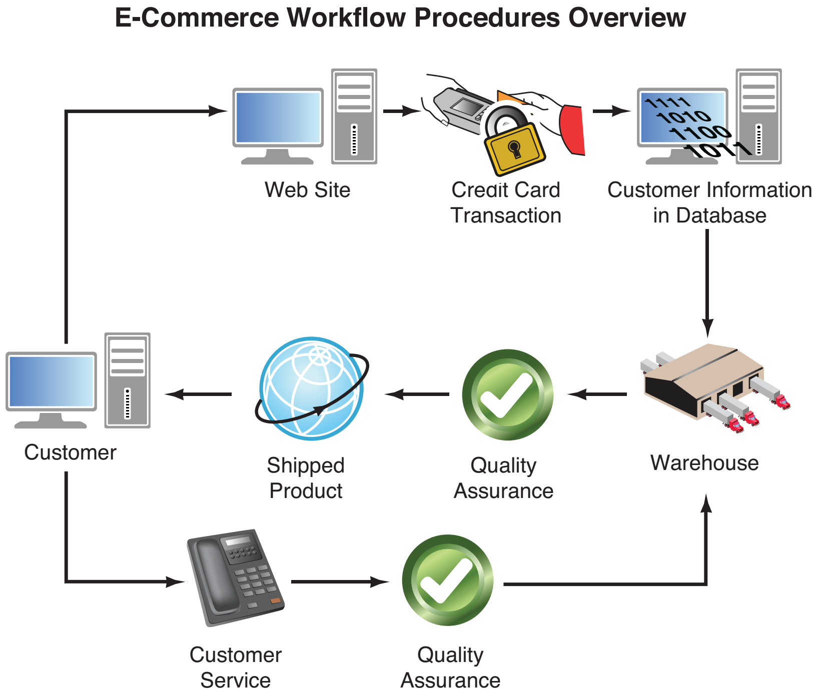


FIGURE 8.1 Example of the graphic format.

A ***flowchart***, shown in Figure 8.2, is a diagrammatic representation of steps in a decision-making process. A flowchart provides an easy-to-follow mechanism for walking a worker through a series of logical decisions and the steps that should be taken as a result. When developing flowcharts, you should use the generally accepted flowchart symbols. ISO 5807:1985 defines symbols to be used in flowcharts and gives guidance for their use.

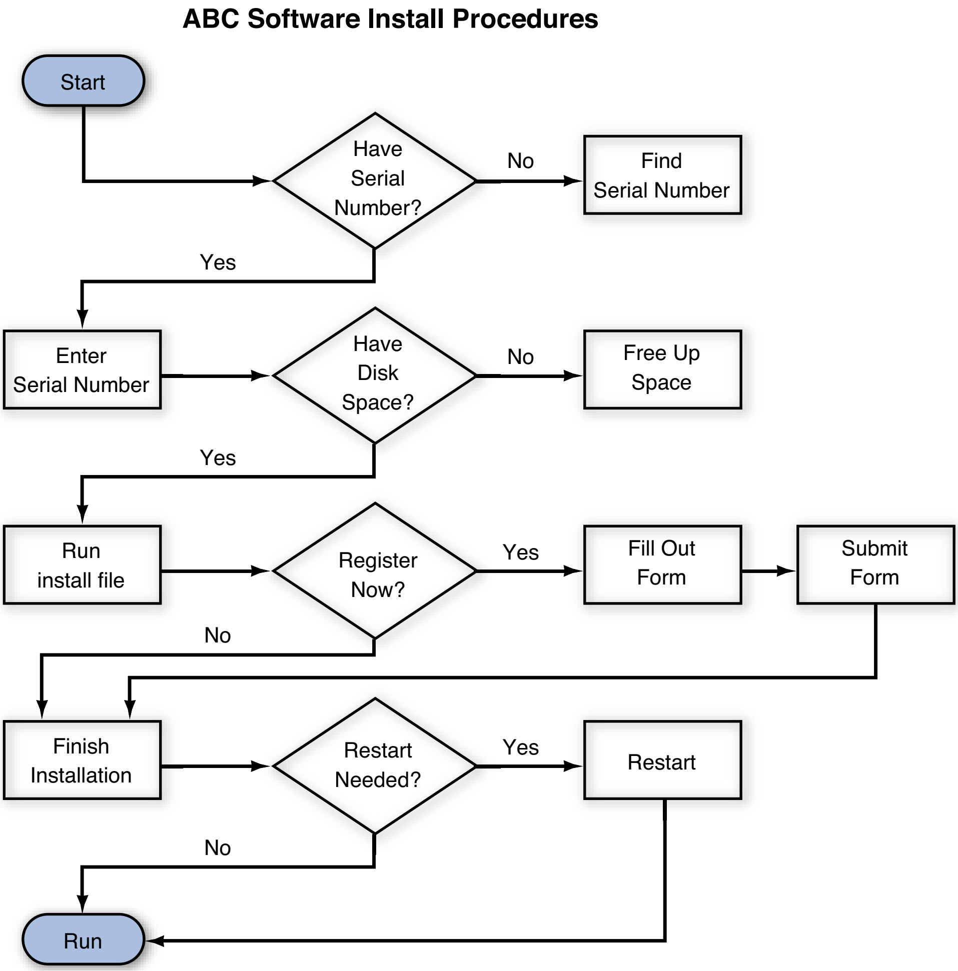


FIGURE 8.2 Flowchart format.

FYI: A Recommended Writing Resource

A recommended resource for learning how to write procedures is *Procedure Writing: Principles and Practices*, Second Edition, by Douglas Wieringa, Christopher Moore, and Valerie Barnes (Battelle Press, 1998, ISBN 1-57477-052-7).

In Practice

Standard Operating Procedures Documentation Policy

Synopsis: Standard operating procedures (SOPs) are required in order to ensure the consistent and secure operation of information systems.

Policy Statement:

- SOPs for all critical information processing activities will be documented.
  - Information system custodians are responsible for developing and testing the procedures.
  - Information system owners are responsible for authorization and ongoing review.
  - The Office of Information Technology is responsible for the publication and distribution of information systems-related SOPs.
- SOPs for all critical information security activities will be documented, tested, and maintained.
  - Information security custodians are responsible for developing and testing the procedures.
  - The Office of Information Security is responsible for authorization, publication, distribution, and review of information security–related SOPs.

Operational Change Control

Operational change is inevitable. ***Change control*** is an internal procedure by which authorized changes are made to software, hardware, network access privileges, or business processes. The information security objective of change control is to ensure the stability of the network while maintaining the required levels of confidentiality, integrity, and availability (CIA). A ***change management process*** establishes an orderly and effective mechanism for submission, evaluation, approval, prioritization, scheduling, communication, implementation, monitoring, and organizational acceptance of change.

Why Manage Change?

The process of making changes to systems in production environments presents risks to ongoing operations and data that are effectively mitigated by consistent and careful management. Consider this scenario: Windows 8 is installed on a mission-critical workstation. The system administrator installs a service pack. A service pack often will make changes to system files. Now imagine that for a reason beyond the installer's control, the process fails halfway through. What is the result? An operating system that is neither the original version, nor the updated version. In other words, there could be a mix of new and old system files, which would result in an unstable platform. The negative impact on the process that depends on the workstation would be significant. Take this example to the next level and imagine the impact if this machine were a network server used by all employees all day long. Consider the impact on the productivity of the entire company if this machine were to become unstable because of a failed update. What if the failed change impacted a customer-facing device? The entire business could come grinding to a halt. What if the failed change also introduced a new vulnerability? The result could be loss of confidentiality, integrity, and/or availability (CIA).

Change needs to be controlled. Organizations that take the time to assess and plan for change spend considerably less time in crisis mode. The change control process starts with an ***RFC (Request for Change)***. The RFC is submitted to a decision-making body (generally senior management). The change is then evaluated and, if approved, implemented. Each step must be documented. Not all changes should be subject to this process. Matter of fact, doing so would negate the desired effect and in the end significantly impact operations. There should be an organization policy that clearly delineates the type(s) of change that the change control process applies to. Additionally, there needs to be a mechanism to implement "emergency" changes.

Submitting an RFC

The first phase of the change control process is an RFC submission. The request should include the following items:

- Requestor name and contact information
- Description of the proposed change
- Justification of why the proposed changes should be implemented
- Impact of not implementing the proposed change
- Alternatives to implementing the proposed change
- Cost
- Resource requirements
- Timeframe

Taking into consideration the preceding information as well as organizational resources, budget, and priorities, the decision makers can choose to continue to evaluate, approve, reject, or defer until a later date.

Developing a Change Control Plan

Once a change is approved, the next step is for the requestor to develop a ***change control plan***. The complexity of the change as well as the risk to the organization will influence the level of detail required. Standard components of a change control plan include a security review to ensure that new vulnerabilities are not being introduced, implementation instructions, rollback and/or recovery options, and post-implementation monitoring.

Communicating Change

The need to communicate to all relevant parties that a change will be taking place cannot be overemphasized. The Prosci Research 2011 Management Best Practices study found that communicating the reason for change was identified as the number-one most important message to share with employees and the second most important message for managers and executives (with the number-one message being about their role and expectations). The messages to communicate to impacted employees fell into two categories: messages about the change and how the change impacts them.

Messages about the change include the following:

- The current situation and the rationale for the change
- A vision of the organization after the change takes place
- The basics of what is changing, how it will change, and when it will change
- The expectation that change will happen and is not a choice
- Status updates on the implementation of the change, including success stories

Messages about how the change will affect the employee include the following:

- The impact of the change on the day-to-day activities of the employee
- Implications of the change on job security
- Specific behaviors and activities expected from the employee, including support of the change
- Procedures for getting help and assistance during the change

Projects that fail to communicate are doomed to fail.

Implementing and Monitoring Change

Once the change is approved, planned, and communicated, it is time to implement. Change can be unpredictable. If possible, the change should first be applied to a test environment and monitored for impact. Even minor changes can cause havoc. For example, a simple change in a shared database's filename could cause all applications that use it to fail. For most environments, the primary implementation objective is to minimize stakeholder impact. This includes having a plan to roll back or recover from a failed implementation.

Throughout the implementation process, all actions should be documented. This includes actions taken before, during, and after the changes have been applied. Changes should not be "set and forget." Even a change that appears to have been flawlessly implemented should be monitored for unexpected impact.

Some emergency situations require organizations to bypass certain change controls in order to recover from an outage, incident, or unplanned event. Especially in these cases, it is important to document the change thoroughly, communicate the change as soon as possible, and have it approved post-implementation.

In Practce

Operational Change Control Policy

Synopsis: To minimize harm and maximize success associated with making changes to information systems or processes.

Policy Statement:

- The Office of Information Technology is responsible for maintaining a documented change control process that provides an orderly method in which changes to the information systems and processes are requested and approved prior to their installation and/or implementation. Changes to information systems include but are not limited to:
  - Vendor-released operating system, software application, and firmware patches, updates, and upgrades
  - Updates and changes to internally developed software applications
  - Hardware component repair/replacement
- Implementations of security patches are exempt from this process as long as they follow the approved patch management process.
- The change control process must take into consideration the criticality of the system and the risk associated with the change.
- Changes to information systems and processes considered critical to the operation of the company must be subject to pre-production testing.
- Changes to information systems and processes considered critical to the operation of the company must have an approved rollback and/or recovery plan.
- Changes to information systems and processes considered critical to the operation of the company must be approved by the Change Management Committee. Other changes may be approved by the Director of Information Systems, Chief Technology Officer (CTO), or Chief Information Officer (CIO).
- Changes must be communicated to all impacted stakeholders.
- In an emergency scenario, changes may be made immediately (business system interruption, failed server, and so on) to the production environment. These changes will be verbally approved by a manager supervising the affected area at the time of change. After the changes are implemented, the change must be documented in writing and submitted to the CTO.

Why Is Patching Handled Differently?

A ***patch*** is software or code designed to fix a problem. Applying ***security patches*** is the primary method of fixing security vulnerabilities in software. The vulnerabilities are often identified by researchers or ethical hackers who then notify the software company so that they can develop and distribute a patch. A function of change management, patching is distinct in how often and how quickly patches need to be applied. The moment a patch is released, attackers make a concerted effort to reverse engineer the patch swiftly (measured in days or even hours), identify the vulnerability, and develop and release exploit code. The time immediately after the release of a patch is ironically a particularly vulnerable moment for most organizations due to the time lag in obtaining, testing, and deploying a patch.

FYI: Patch Tuesday and Exploit Wednesday

Microsoft releases new security updates and their accompanying bulletins on the second Tuesday of every month at approximately 10 a.m. Pacific Time, hence the name ***Patch Tuesday***. The following day is referred to as ***Exploit Wednesday***, signifying the start of exploits appearing in the wild.

Understanding Patch Management

Timely patching of security issues is generally recognized as critical to maintaining the operational CIA of information systems. ***Patch management*** is the process of scheduling, testing, approving, and applying security patches. Vendors who maintain information systems within a company network should be required to adhere to the organizational patch management process.

The patching process can be unpredictable and disruptive. Users should be notified of potential downtime due to patch installation. Whenever possible, patches should be tested prior to enterprise deployment. However, there may be situations where it is prudent to waive testing based on the severity and applicability of the identified vulnerability. If a critical patch cannot be applied in a timely manner, senior management should be notified of the risk to the organization.

NIST Special Publication 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, published July 2013, is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. The publication also provides an overview of enterprise patch management technologies and discusses metrics for measuring the technologies' effectiveness and for comparing the relative importance of patches.

In Practice

Security Patch Management Policy

Synopsis: The timely deployment of security patches will reduce or eliminate the potential for exploitation.

Policy Statement:

- Implementations of security patches are exempt from the organizational change management process as long as they follow the approved patch management process.

- The Office of Information Security is responsible for maintaining a documented patch management process.
- The Office of Information Technology is responsible for the deployment of all operating system, application, and device security patches.
  - Security patches will be reviewed and deployed according to applicability of the security vulnerability and/or identified risk associated with the patch or hotfix.
  - Security patches will be tested prior to deployment in the production environment. The CIO and the CTO have authority to waive testing based on the severity and applicability of the identified vulnerability.
- Vendors who maintain company systems are required to adhere to the company patch management process.
- If a security patch cannot be successfully applied, the COO must be notified. Notification must detail the risk to the organization.

Malware Protection

Malware, short for "malicious software," is software (or script or code) designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems and mobile devices. Malware is operating system agnostic. Malware can infect systems by being bundled with other programs or self-replicating however; the vast majority of malware requires user interaction such as clicking an email attachment or downloading a file from the Internet. It is critical that s***ecurity awareness*** programs articulate individual responsibility in fighting malware.

Malware has become the tool of choice for cybercriminals, hackers, and hacktivists. It has become easy for attackers to create their own malware by acquiring malware toolkits, such as Zeus, SpyEye, and Poison Ivy, and customizing the malware produced by those toolkits to meet their individual needs. Many of these toolkits are available for purchase, whereas others are open source, and most have user-friendly interfaces that make it simple for unskilled attackers to create customized, high-capability malware. Unlike most malware several years ago, which tended to be easy to notice, much of today's malware is specifically designed to quietly, slowly spread to other hosts, gathering information over extended periods of time and eventually leading to exfiltration of sensitive data and other negative impacts. The term ***advanced persistent threats (APTs)*** is generally used to refer to this approach.

NIST Special Publication 800-83, Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, published in July 2012, provides recommendations for improving an organization's malware incident prevention measures. It also gives extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones.

Are There Different Types of Malware?

Malware categorization is based on infection and propagation characteristics. The categories of malware include viruses, worms, Trojans, bots, ransomware, rootkits, and spyware/adware. ***Hybrid malware*** is code that combines characteristics of multiple categories—for example, combining a virus' ability to alter program code with a worm's ability to reside in live memory and to propagate without any action on the part of the user.

A ***virus*** is malicious code that attaches to and becomes part of another program. Generally, viruses are destructive. Almost all viruses attach themselves to executable files. They then execute in tandem with the host file. Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected email attachments. One of the most famous examples of a virus outbreak was the Melissa virus (also known as Mailissa, Simpsons, Kwyjibo, and Kwejeebo), which was first identified on March 26, 1999. Melissa was distributed as an email attachment that, when opened, disabled a number of safeguards and, if the user had the Microsoft Outlook email program, caused the virus to be re-sent to the first 50 people in each of the user's address books. Melissa caused Microsoft to shut down incoming email. Intel, Dell, and a number of federal agencies reported being affected.

A ***worm*** is a piece of malicious code that can spread from one computer to another without requiring a host file to infect. Worms are specifically designed to exploit known vulnerabilities, and they spread by taking advantage of network and Internet connections. As of 2013, the 2003 worm W32/SQL Slammer (aka Slammer and Sapphire) still holds the record for the fastest spreading worm. It infected the process space of Microsoft SQL Server 2000 and Microsoft SQL Desktop Engine (MSDE) by exploiting an unpatched buffer overflow. Once running, the worm tried to send itself to as many other Internet-accessible SQL hosts as possible. Microsoft had released a patch six months prior to the Slammer outbreak.

A ***Trojan*** is malicious code that masquerades as a legitimate benign application. For example, when a user downloads a game, he may get more than he expected. The game may serve as a conduit for a malicious utility such as a keylogger or screen scraper. A ***keylogger*** is designed to capture and log keystrokes, mouse movements, Internet activity, and processes in memory such as print jobs. A ***screen scraper*** makes copies of what you see on your screen. A typical activity attributed to Trojans is to open connections to a ***command and control server*** (known as a C&C). Once the connection is made, the machine is said to be "owned." The attacker takes control of the infected machine. In fact, cybercriminals will tell you that once they have successfully installed a Trojan on a target machine, they actually have more control over that machine than the very person seated in front of and interacting with it. Once "owned," access to the infected device may be sold to other criminals. Trojans do not reproduce by infecting other files, nor do they self-replicate. Trojans must spread through user interaction, such as opening an email attachment or downloading and running a file from the Internet. Examples of Trojans include Zeus and SpyEye. Both Trojans are designed to capture financial website login credentials and other personal information.

Bots (also known as *robots*) are snippets of code designed to automate tasks and respond to instructions. Bots can self-replicate (like worms) or replicate via user action (like Trojans). A malicious bot is installed in a system without the user's permission or knowledge. The bot connects back to a central server or command center. An entire network of compromised devices is known as a ***botnet***. One of the most common uses of a botnet is to launch distributed denial of service (DDoS) attacks.

Ransomware is a type of malware that takes a computer or its data hostage in an effort to extort money from victims. There are two types of ransomware: *Lockscreen ransomware* displays a full-screen image or web page that prevents you from accessing anything in your computer. *Encryption ransomware* encrypts your files with a password, preventing you from opening them. The most common ransomware scheme is a notification that authorities have detected illegal activity on your computer and you must pay a "fine" to avoid prosecution and regain access to your system.

A ***rootkit*** is a set of software tools that hides its presence in the lower layers of the operating system's application layer, the operating system kernel, or in the device basic input/output system (BIOS) with privileged access permissions. *Root* is a Unix/Linux term that denotes administrator-level or privileged access permissions. The word *kit* denotes a program that allows someone to obtain root/admin-level access to the computer by executing the programs in the kit—all of which is done without end-user consent or knowledge. The intent is generally remote C&C. Rootkits cannot self-propagate or replicate; they must be installed on a device. Because of where they operate, they are very difficult to detect and even more difficult to remove.

Spyware is a general term used to describe software that without a user's consent and/or knowledge tracks Internet activity such as searches and web surfing, collects data on personal habits, and displays advertisements. Spyware sometimes affects the device configuration by changing the default browser, changing the browser home page, or installing "add-on" components. It is not unusual for an application or online service license agreement to contain a clause that allows for the installation of spyware.

FYI: Do-Not-Track Legislation

As of the writing of this text, Congress has failed to pass S. 418: Do-Not-Track Online Act of 2013. The proposed legislation requires the Federal Trade Commission to establish and enforce (1) regulations that establish standards for the implementation of a mechanism by which an individual can indicate whether he or she prefers to have personal information collected by providers of online services, including by providers of mobile applications and services, and (2) rules that prohibit such providers from collecting personal information on individuals who have expressed a preference not to have such information collected.

The advertising and direct marketing industries have lobbied hard to block passage of this bill. In response, Microsoft, Apple, and Google are working on browser-based controls that would allow a user to disable cookies and spyware. However, advertisers are lobbying Congress to legislate that consumers be required to choose whether they want cookies blocked or not. Under those proposals, tracking would be on by default and consumers would have to choose to turn it off.

For more information, visit www.govtrack.us/congress/bills/113/s418.

How Is Malware Controlled?

The IT department is generally tasked with the responsibility of employing a strong anti-malware defense-in-depth strategy. In this case, ***defense in depth*** means implementing prevention, detection, and response controls, coupled with a security awareness campaign.

Using Prevention Controls

The goal of ***prevention control*** is to stop an attack before it even has a chance to start. This can be done in a number of ways:

- Impact the distribution channel by training users not to clink links embedded in email, open unexpected email attachments, irresponsibly surf the Web, download games or music, participate in peer-to-peer (P2P) networks, and allow remote access to their desktop.
- Configure the firewall to restrict access.
- Do not allow users to install software on company-provided devices.
- Do not allow users to make changes to configuration settings.
- Do not allow users to have administrative rights to their workstations. Malware runs in the security context of the logged-in user.
- Do not allow users to disable (even temporarily) anti-malware software and controls.
- Disable remote desktop connections.
- Apply operating system and application security patches expediently.
- Enable browser-based controls, including pop-up blocking, download screening, and automatic updates.
- Implement an enterprise-wide antivirus/anti-malware application. It is important that the anti-malware solutions be configured to update as frequently as possible because many new pieces of malicious code are released daily.

Using Detection Controls

Detection controls should identify the presence of malware, alert the user (or network administrator), and in the best-case scenario stop the malware from carrying out its mission. Detection should occur at multiple levels—at the entry point of the network, on all hosts and devices, and at the file level. Detection controls include the following:

- Real-time firewall detection of suspicious file downloads.
- Real-time firewall detection of suspicious network connections.
- Host and network-based intrusion detection systems or intrusion prevention systems (IDS/IPS).

- Review and analysis of firewalls, IDS, operating systems, and application logs for indicators of compromise.
- User awareness to recognize and report suspicious activity.
- Help desk (or equivalent) training to respond to malware incidents.

What Is Antivirus Software?

Antivirus (AV) software is used to detect, contain, and in some cases eliminate malicious software. Most AV software employs two techniques—signature-based recognition and behavior-based (heuristic) recognition. A common misconception is that AV software is 100% effective against malware intrusions. Unfortunately, that is not the case. Although AV applications are an essential control, they are increasingly limited in their effectiveness. This is due to three factors—the sheer volume of new malware, the phenomena of "single-instance" malware, and the sophistication of blended threats.

The core of AV software is known as the "engine." It is the basic program. The program relies on virus definition files (known as DAT files) to identify malware. The definition files must be continually updated by the software publisher and then distributed to every user. This was a reasonable task when the number and types of malware were limited. New versions of malware are increasing exponentially, thus making research, publication, and timely distribution a next-to-impossible task. In their 2013 "State of Malware" report, McAfee Labs researchers announced that they are cataloging upwards of 100,000 new malware samples each day—that is 69 new pieces of malware a minute or about one new threat every second. Complicating this problem is the phenomena of single-instance malware—that is, variants only used one time. The challenge here is that DAT files are developed using historical knowledge, and it is impossible to develop a corresponding DAT file for a single instance that has never been seen before. The third challenge is the sophistication of malware—specifically, blended threats. A ***blended threat*** occurs when multiple variants of malware (worms, viruses, bots, and so on) are used in concert to exploit system vulnerabilities. Blended threats are specifically designed to circumvent AV and behavioral-based defenses.

FYI: W32.Stuxnet: A Complex Blended Threat

Stuxnet, which was developed by the governments of the United States and Israel, is a good example of a complex blended threat. W32.Stuxnet was designed to target and disrupt industrial control systems. Stuxnet malware was initially introduced via a USB device connected to a target computer. Once executed, the malware searched for one of four different Windows vulnerabilities, which enabled it to install a rootkit. From there, worm techniques spread the malicious code to as many computers within the network as possible. The malware updated itself through a P2P mechanism. Stuxnet also had a separate module that used worm techniques to look for supervisory control and data acquisition (SCADA) controller devices manufactured by Siemens. When Stuxnet located one of these devices, it installed yet another piece of malicious code that was designed to control or at least disrupt the device's operation. Then encrypted VPN tunneling was used to connect to two websites, which issued commands from and reported to the perpetrators of the attack.

In Practice

Malicious Software Policy

Synopsis: To ensure a company-wide effort to prevent, detect, and contain malicious software.

Policy Statement:

- The Office of Information Technology is responsible for recommending and implementing prevention, detection, and containment controls. At a minimum,
  - Anti-malware software will be installed on all computer workstations and servers to prevent, detect, and contain malicious software.
  - Any system found to be out of date with vendor-supplied virus definition and/or detection engines must be documented and remediated immediately or disconnected from the network until it can be updated.
- The Office of Human Resources is responsible for developing and implementing malware awareness and incident reporting training.
- All malware-related incidents must be reported to the Office of Information Security.
- The Office of Information Security is responsible for incident management.

Data Replication

The impact of malware, computer hardware failure, accidental deletion of data by users, and other eventualities is reduced with an effective data backup or replication process that includes periodic testing to ensure the integrity of the data as well as the efficiency of the procedures to restore that data in the production environment. Having multiple copies of data is essential for both data integrity and availability. ***Data replication*** is the process of copying data to a second location that is available for immediate or near-time use. ***Data backup*** is the process of copying and storing data that can be restored to its original location. A company that exists without a tested backup-and-restore or data replication solution is like a flying acrobat working without a net.

Is There a Recommended Backup or Replication Strategy?

Making the decision to back up or to replicate, and how often, should be based on the impact of not being able to access the data either temporarily or permanently. Strategic, operational, financial, transactional, and regulatory requirements must be considered. You should consider several factors when designing a replication or data backup strategy. Reliability is paramount; speed and efficiency are also very important, as are simplicity, ease of use, and, of course, cost. These factors will all define the criteria for the type and frequency of the process.

Backed-up or replicated data should be stored at an off-site location, in an environment where it is secure from theft, the elements, and natural disasters such as floods and fires. The backup strategy and associated procedures must be documented.

FYI: Cloud Storage

"The cloud" is a metaphor for the Internet. ***Cloud storage*** refers to using Internet-based resources to store your data. A number of the cloud-based computing vendors such as Google and Amazon offer scalable, affordable storage options that can be used in place of (or in addition to) local backup.

Understanding the Importance of Testing

The whole point of replicating or backing up data is that it can be accessed or restored if the data is lost or tampered with. In other words, the value of the backup or replication is the assurance that running a restore operation will yield success and that the data will once again be available for production and business-critical application systems.

Just as proper attention must be paid to designing and testing the replication or backup solution, the accessibility or restore strategy must also be carefully designed and tested before being approved. Accessibility or restore procedures must be documented. The only way to know whether a replication or backup operation was successful and can be relied upon is to test it. It is recommended that test access or restores of random files be conducted at least monthly.

In Practice

Data Replication Policy

Synopsis: Maintain the availability and integrity of data in the case of error, compromise, failure, or disaster.

Policy Statement:

- The Office of Information Security is responsible for the design and oversight of the enterprise replication and backup strategy. Factors to be considered include but are not limited to impact, cost, and regulatory requirements.
- Data contained on replicated or backup media will be protected at the same level of access control as the data on the originating system.
- The Office of Information Technology is responsible for the implementation, maintenance, and ongoing monitoring of the replication and backup/restoration strategy.
  - The process must be documented.
  - The procedures must be tested on a scheduled basis.
- Backup media no longer in rotation for any reason will be physically destroyed so that the data is unreadable by any means.

Secure Messaging

In 1971, Ray Tomlinson, a Department of Defense (DoD) researcher, sent the first ARPANET email message to himself. The ***ARPANET***, the precursor to the Internet, was a United States (U.S.) Advanced Research Project Agency (ARPA) project intended to develop a set of communications protocols to transparently connect computing resources in various geographical locations. Messaging applications were available on ARPANET systems; however, they could only be used for sending messages to users with local system accounts. Tomlinson modified the existing messaging system so that users could send messages to users on other ARPANET-connected systems. After Tomlinson's modification was available to other researchers, email quickly became the most heavily used application on the ARPANET. Security was given little consideration because the ARPANET was viewed as a trusted community.

Current email architecture is strikingly similar to the original design. Consequently, email servers, email clients, and users are vulnerable to exploit and are frequent targets of attack. Organizations need to implement controls that safeguard the CIA of email hosts and email clients. NIST Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, published in February 2007, recommends security practices for designing, implementing, and operating email systems on public and private networks.

What Makes Email a Security Risk?

When you send an email, the route it takes in transit is complex, with processing and sorting occurring at several intermediary locations before arriving at the final destination. In its native form, email is transmitted using clear text protocols. It is almost impossible to know if anyone has read or manipulated your email in transit. Forwarding, copying, storing, and retrieving email is easy (and commonplace); preserving confidentiality of the contents and metadata is difficult. Additionally, email can be used to distribute malware and to exfiltrate company data.

Understanding Clear Text Transmission

Simple Mail Transfer Protocol (SMTP) is the de facto message transport standard for sending email messages. Jon Postel of the University of Southern California developed SMTP in August 1982. At the most basic level, SMTP is a minimal language that defines a communications protocol for delivering email messages. Once a message is delivered, users need to access the mail server to retrieve the message. The two most widely supported mailbox access protocols are ***Post Office Protocol (now POP3)***, developed in 1984, and ***Internet Message Access Protocol (IMAP)***, developed in 1988. The designers never envisioned that someday email would be ubiquitous, and as with the original ARPANET communications, reliable message delivery, rather than security, was the focus. SMTP, POP, and IMAP are all clear-text protocols. This means that the delivery instructions (including access passwords) and email contents are transmitted in a human readable form. Information sent in clear text may be captured and read by third parties, resulting in a breach of confidentiality. Information sent in clear text may be captured and manipulated by third parties, resulting in a breach of integrity.

Encryption protocols can be used to protect both authentication and contents. ***Encryption*** protects the privacy of the message by converting it from (readable) plaintext into (scrambled) cipher text. We will be examining encryption protocols in depth in Chapter 10, "Information Systems Acquisition, Development, and Maintenance." Encrypted email is often referred to as "secure email." As we discussed in Chapter 5, "Asset Management," email-handling standards should specify the email encryption requirements for each data classification. Most email encryption utilities can be configured to auto-encrypt based on preset criteria, including content, recipient, and email domain.

Understanding Metadata

Documents sent as email attachments might contain more information than the sender intended to share. The files created by many office programs contain hidden information about the creator of the document, and may even include some content that has been reformatted, deleted, or hidden. This information is known as ***metadata***.

Keep this in mind in the following situations:

- If you recycle documents by making changes and sending them to new recipients (that is, using a boilerplate contract or a sales proposal).
- If you use a document created by another person. In programs such as Microsoft Office, the document might list the original person as the author.
- If you use a feature for tracking changes. Be sure to accept or reject changes, not just hide the revisions.

Understanding Embedded Malware

Email is an effective method to attack and ultimately infiltrate an organization. Common mechanisms include embedding malware in an attachment and directing the recipient to click a hyperlink that connects to a malware distribution site (unbeknownst to the user). Increasingly, attackers are using email to deliver zero-day attacks at targeted organizations. A ***zero-day exploit*** is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes publicly or generally known.

Malware can easily be embedded in common attachments such as PDF, Word, and Excel files or even a picture. Not allowing any attachments would simplify email security; however, it would dramatically reduce the usefulness of email. Determining which types of attachments to allow and which to filter out must be an organizational decision. Filtering is a mail server function and is based on the file type. The effectiveness of filtering is limited because attackers can modify the file extension. In keeping with a defense-in-depth approach, allowed attachments should be scanned for malware at the mail gateway, email server, and email client.

A ***hyperlink*** is a word, phrase, or image that is programmatically configured to connect to another document, bookmark, or location. Hyperlinks have two components—the text to display (such as www.goodplace.com) and the connection instructions. Genuine-looking hyperlinks are used to trick email recipients into connecting to malware distribution sites. Most email client applications have the option to disable active hyperlinks. The challenge here is that hyperlinks are often legitimately used to direct the recipient to additional information. In both cases, users need to be taught to not click on links or open any attachment associated with an unsolicited, unexpected, or even mildly suspicious email.

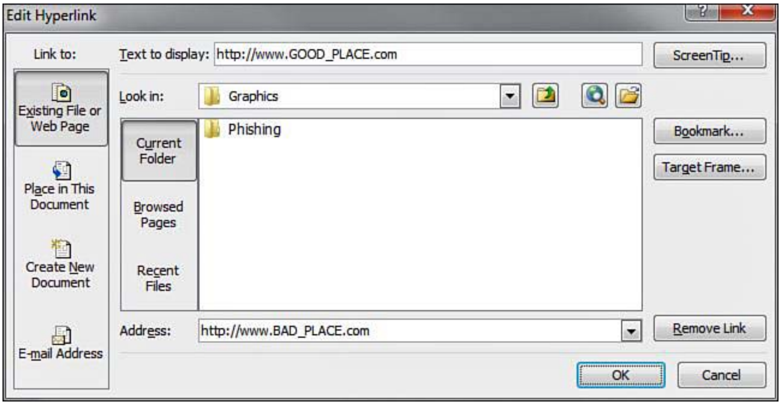
Controlling Access to Personal Email Applications

Access to personal email accounts should not be allowed from a corporate network. Email that is delivered via personal email applications such as Gmail bypass all of the controls that the company has invested in, such as email filtering and scanning. A fair comparison would be that you install a lock, lights, and an alarm system on the front door of your home but choose to leave the back door wide open all the time based on the assumption that the back door is really just used occasionally for friends and family.

In addition to outside threats, consideration needs to be given to both the malicious and unintentional insider threat. If an employee decides to correspond with a customer via personal email or if an employee chooses to exfiltrate information and send it via personal email, there would be no record of the activity. From both an HR and a forensic perspective, this would hamper an investigation and subsequent response.

FYI: Fraudulent Hyperlinks

Creating a fraudulent hyperlink is easy. You can use HTML code or built-in commands. Figure 8.3 is from a Microsoft Office application. Notice the two boxes—Text to Display (Good_Place.com) and Address (pointing to Bad_Place.com). There is no requirement that the two match!



Edit Hyperlink

Text to display: http://www.GOOD_PLACE.com

Look in: Graphics

Phishing

Address: http://www.BAD_PLACE.com

FIGURE 8.3 Editing a hyperlink.

Understanding Hoaxes

Every year, a vast amount of money is lost, in the form of support costs and equipment workload, due to hoaxes sent by email. A ***hoax*** is a deliberately fabricated falsehood. An email hoax may be a fake virus warning or false information of a political or legal nature, and often borders on criminal mischief. Some hoaxes ask recipients to take action that turns out to be damaging—deleting supposedly malicious files from their local computer, sending uninvited mail, randomly boycotting organizations for falsified reasons, or defaming an individual or group by forwarding the message on.

Understanding the Risks Introduced by User Error

The three most common user errors that impact the confidentiality of email are sending email to the wrong person, choosing "Reply All" instead of "Reply," and using "Forward" inappropriately.

It is easy to mistakenly send email to the wrong address. This is especially true with email clients that auto-complete addresses based on the first three or four characters entered. All users must be made aware of this, and must pay strict attention to the email address entered in the To field, along with the CC and BCC fields when used.

The consequence of choosing Reply All instead of Reply can be significant. The best-case scenario is embarrassment. In the worst cases, confidentiality is violated by distributing information to those who do not have a "need to know." In regulated sectors such as healthcare and banking, violating the privacy of patients and/or clients is against the law.

Forwarding has similar implications. Assume that two people have been emailing back and forth using the "reply" function. Their entire conversation can be found online. Now suppose that one of them decides that something in the last email is of interest to a third person and forwards the email. In reality, what that person just did was forward the entire thread of emails that had been exchanged between the two original people. This may well have not been the person's intent and may violate the privacy of the other original correspondent.

Are Email Servers at Risk?

Email servers are hosts that deliver, forward, and store email. Email servers are attractive targets because they are a conduit between the Internet and the internal network. Protecting an email server from compromise involves hardening the underlying operating system, the email server application, and the network to prevent malicious entities from directly attacking the mail server. Email servers should be single-purpose hosts, and all other services should be disabled or removed. Email server threats include relay abuse and DoS attacks.

Understanding Relay Abuse and Blacklisting

The role of an email server is to process and relay email. The default posture for many email servers is to process and relay *any* mail sent to the server. This is known as ***open mail relay***. The ability to relay mail through a server can (and often is) taken advantage of by those who benefit from the illegal use of the resource. Criminals conduct Internet searches for email servers configured to allow relay. Once they locate an open relay server, they use it for distributing spam and malware. The email appears to come from the company whose email server was misappropriated. Criminals use this technique to hide their identity. This is not only an embarrassment but can also result in legal and productivity ramifications.

In a response to the deluge of spam and email malware distribution, blacklisting has become a standard practice. A ***blacklist*** is a list of email addresses, domain names, or IP addresses known to send unsolicited commercial email (spam) or email-embedded malware. The process of blacklisting is to use the blacklist as an email filter. The receiving email server checks the incoming emails against the blacklist, and when a match is found, the email is denied.

Understanding Denial of Service Attacks

The SMTP protocol is especially vulnerable to DDoS attacks because, by design, it accepts and queues incoming emails. To mitigate the effects of email DoS attacks, the mail server can be configured to limit the amount of operating system resources it can consume. Some examples include configuring the mail server application so that it cannot consume all available space on its hard drives or partitions, limiting the size of attachments that are allowed, and ensuring log files are stored in a location that is sized appropriately.

In Practice

Email and Email Systems Security Policy

Synopsis: To recognize that email and messaging platforms are vulnerable to disclosure and attack, and to assign responsibility to safeguarding said systems.

Policy Statement:

- The Office of Information Security is responsible for assessing the risk associated with email and email systems. Risk assessments must be performed at a minimum bi-annually or whenever there is a change trigger.
- The Office of Information Security is responsible for creating email security standards, including but not limited to attachment and content filtering, encryption, malware inspection, and DDoS mitigation.
- External transmission of data classified as “protected” or “confidential” must be encrypted.
- Remote access to company email must conform to the corporate remote access standards.
- Access to personal web-based email from the corporate network is not allowed.
- The Office of Information Technology is responsible for implementing, maintaining, and monitoring appropriate controls.
- The Office of Human Resources is responsible for providing email security user training.

Activity Monitoring and Log Analysis

NIST defines a ***log*** as a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network. Security logs are generated by many sources, including security software, such as AV software, firewalls, and IDS/IPS systems; operating systems on servers, workstations, and networking equipment; and applications. Logs are a key resource when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Third-party security specialists should be engaged for log analysis if in-house knowledge is not sufficient.

What Is Log Management?

Log management activities involve configuring the log sources, including log generation, storage, and security, performing analysis of log data, initiating appropriate responses to identified events, and managing the long-term storage of log data. Log management infrastructures are typically based on one of the two major categories of log management software: syslog-based centralized logging software and security information and event management software (SIEM). ***Syslog*** provides an open framework based on message type and severity. ***Security information and event management*** (SIEM) software includes commercial applications and often uses proprietary processes. NIST Special Publication SP 800-92, *Guide to Computer Security Log Management*, published September 2006, provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. The guidance in SP 800-92 covers several topics, including establishing a log management infrastructure.

Prioritizing and Selecting Which Data to Log

Ideally, data would be collected from every significant device and application on the network. The challenge is that network devices and applications can generate hundreds of events per minute. A network with even a small number of devices can generate millions of events per day. The sheer volume can overwhelm a log management program. Prioritization and inclusion decisions should be based on system or device criticality, data protection requirements, vulnerability to exploit, and regulatory requirements. For example, websites and servers that serve as the public face of the company are vulnerable specifically because they are Internet accessible. E-commerce application and database servers may drive the company's revenue and are targeted because they contain valuable information such as credit card information. Internal devices are required for day-to-day productivity; access makes them vulnerable to insider attacks. In addition to identifying suspicious activity, attacks, and compromises, log data can be used to better understand normal activity, provide operational oversight, and provide a historical record of activity. The decision-making process should include information system owners as well as information security, compliance, legal, HR, and IT personnel.

Analyzing Logs

Done correctly and consistently, log analysis is a reliable and accurate way to discover potential threats, identify malicious activity, and provide operational oversight. Log analysis techniques include correlation, sequencing, signature, and trend analysis:

- ***Correlation*** ties individual log entries together based on related information.
- ***Sequencing*** examines activity based on patterns.
- ***Signature*** compares log data to "known bad" activity.
- ***Trend analysis*** identifies activity over time that in isolation might appear normal.

A common mistake made when analyzing logs is to focus on "denied" activity. Although it is important to know what was denied, it is much more important to focus on allowed activity that may put the organization at risk.

FYI: Log Review Regulatory Requirements and Contractual Obligations

Monitoring event and audit logs is an integral part of complying with a variety of federal regulations, including the Gramm-Leach-Bliley Act. In addition, as of July 2013, at least 48 states and U.S. territories have instituted security breach notification laws that require businesses to monitor and protect specific sets of consumer data:

- ***Gramm-Leach-Bliley Act (GLBA)*** requires financial institutions to protect their customers' information against security threats. Log management can be helpful in identifying possible security violations and resolving them effectively.
- ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)*** includes security standards for certain health information, including the need to perform regular reviews of audit logs and access reports. Section 4.22 specifies that documentation of actions and activities needs to be retained for at least six years.
- ***Federal Information Security Management Act of 2002 (FISMA)*** requirements found in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, describes several controls related to log management, including the generation, review, protection, and retention of audit records, as well as the actions to be taken because of audit failure.
- ***Payment Card Industry Data Security Standard (PCI DSS)*** applies to organizations that store, process or transmit cardholder data for payment cards. The fifth core PCI DSS principle, *Regulatory Monitor and Test Networks*, includes the requirement to track and monitor all access to network resources and cardholder data.

Firewall logs can be used to detect security threats such as network intrusion, virus attacks, DoS attacks, anomalous behavior, employee web activities, web traffic analysis, and malicious insider activity. Reviewing log data provides oversight of firewall administrative activity and change management, including an audit trail of firewall configuration changes. Bandwidth monitoring can provide information about sudden changes that may be indicative of an attack.

Web server logs are another rich source of data to identify and thwart malicious activity. HTTP status codes indicating redirection, client error, or server error can indicate malicious activity as well as malfunctioning applications or bad HTML code. Checking the logs for Null Referrers can identify hackers who are scanning the website with automated tools that do not follow proper protocols. Log data can also be used to identify web attacks, including SQL injection, cross-site scripting (XSS), and directory traversal. As with the firewall, reviewing web server log data provides oversight of web server/website administrative activity and change management, including an audit trail of configuration changes.

Authentication server logs document user, group, and administrative account activity. Activity that should be mined and analyzed includes account lockouts, invalid account logons, invalid passwords, password changes, and user management changes, including new accounts and changed accounts, computer management events (such as when audit logs are cleared or computer account names are changed), group management events (such as the creation or deletion of groups and the addition of users to high-security groups), and user activity outside of logon time restrictions. Operational activity, such as the installation of new software, the success/failure of patch management, server reboots, and policy changes, should be on the radar as well.

In Practice

Security Log Management Policy

Synopsis: To require that devices, systems, and applications support logging and to assign responsibility for log management.

Policy Statement:

- Devices, systems, and applications implemented by the company must support the ability to log activities, including data access and configuration modifications. Exceptions must be approved by the COO.
- Access to logs must be restricted to individuals with a need-to-know.
- Logs must be retained for a period of 12 months.
- Log analysis reports must be retained for 36 months.
- The Office of Information Security is responsible for:
  - Developing log management standards, procedures, and guidelines
  - Prioritizing log management appropriately throughout the organization
  - Creating and maintaining a secure log management infrastructure
  - Establishing log analysis incident response procedures
  - Providing proper training for all staff with log management responsibilities

- The Office of Information Technology is responsible for:
  - Managing and monitoring the log management infrastructure
  - Proactively analyzing log data to identify ongoing activity and signs of impending problems
  - Providing reports to the Office of Information Security

Service Provider Oversight

Many companies outsource some aspect of their operations. These relationships, however beneficial, have the potential to introduce vulnerabilities. From a regulatory perspective, you can outsource the work but you cannot outsource the legal responsibility. Organizational CIA requirements must extend to all service providers and business partners that store, process, transmit, or access company data and information systems. Third-party controls must be required to meet or, in some cases, exceed internal requirements. When working with service providers, organizations need to exercise due diligence in selecting providers, contractually obligate providers to implement appropriate security controls, and monitor service providers for ongoing compliance with contractual obligations.

FYI: Outsourcing Technology Services Guidance

The Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) *Outsourcing Technology Services Booklet* was published in 2004 with the objective of providing guidance and examination procedures to assist examiners and bankers in evaluating a financial institution's risk management processes to establish, manage, and monitor IT outsourcing relationships. However, the guidance is useful for organizations of all types and sizes. A number of the recommendations in this section are from the FFIEC guidance. To download the booklet from the FFIEC site, visit http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.

What Is Due Diligence?

Vendor ***due diligence*** describes the process or methodology used to assess the adequacy of a service provider. The depth and formality of the due diligence performed may vary based on the risk of the outsourced relationship. Due diligence investigation may include the following:

- Corporate history
- Qualifications, backgrounds, and reputations of company principals
- Financial status, including reviews of audited financial statements
- Service delivery capability, status, and effectiveness

- Technology and systems architecture
- Internal controls environment, security history, and audit coverage
- Legal and regulatory compliance, including any complaints, litigation, or regulatory actions
- Reliance on and success in dealing with third-party service providers
- Insurance coverage
- Incident response capability
- Disaster recovery and business continuity capability

Documentation requested from a service provider generally includes financial statements, security-related policies, proof of insurance, subcontractor disclosure, disaster recovery, and continuity of operations plan, incident notification, and response procedures, security testing results, and independent audit reports such as an SSAE16.

Understanding Independent Audit Reports

The objective of an independent audit is to objectively evaluate the effectiveness of operational, security, and compliance controls. Standards for Attestation Engagements (SSAE) 16, known as ***SSAE16 audit reports***, have become the most widely accepted due diligence documentation. Developed by the American Institute of CPAs (AICPA), there are three audit options: SOC1, SOC2, and SOC3. ***SOC*** is an acronym for controls at a service organization. SOC1 reports focus solely on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. SOC2 and SOC3 reports specifically address one or more of the following five key system attributes:

- **Security**—The system is protected against unauthorized access (both physical and logical).
- **Availability**—The system is available for operation and use as committed or agreed.
- **Processing integrity**—System processing is complete, accurate, timely, and authorized.
- **Confidentiality**—Information designated as confidential is protected as committed or agreed.
- **Privacy**—Personal information is collected, used, retained, disclosed, and disposed of in conformity with the commitments in the entity's privacy notice, and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by the AICPA and Canadian Institute of Chartered Accountants.

SSAE audits must be attested to by a certified public accounting (CPA) firm. SSAE Service organizations that had an SOC 1, SOC 2, or SOC 3 engagement within the past year may register with the AICPA to display the applicable logo.

What Should Be Included in Service Provider Contracts?

Service provider contracts should include a number of information security–related clauses, including performance standards, security and privacy compliance requirements, incident notification, business continuity, disaster recovery commitments, and auditing options. The objective is to ensure that the service provider exercises ***due care***, which is the expectation that reasonable efforts will be made to avoid harm and minimize risk.

Performance standards define minimum service level requirements and remedies for failure to meet standards in the contract—for example, system uptime, deadlines for completing batch processing, and number of processing errors. MTTR (or mean time to repair) may be a clause condition in a service level agreement (SLA), along with a standard reference to Tier 1, Tier 2, and Tier 3 performance factors. Security and privacy compliance requirements address the service provider stewardship of information and information systems as well as organizational processes, strategies, and plans. At a minimum, the service provider control environment should be consistent with organizational policies and standards. The agreement should prohibit the service provider and its agents from using or disclosing the information, except as necessary for or consistent with providing the contracted services, and to protect against unauthorized use. If the service provider stores, processes, receives, or accesses non-public personal information (NPPI), the contract should state that the service provider would comply with all applicable security and privacy regulations.

Incident notification requirements should be clearly spelled out. In keeping with state breach notification laws, unless otherwise instructed by law enforcement, the service provider must disclose both verified security breaches and suspected incidents. The latter is often a point of contention. The contract should specify the timeframe for reporting as well as the type of information that must be included in the incident report.

Lastly, the contract should include the types of audit reports it is entitled to receive (for example, financial, internal control, and security reviews). The contract should specify the audit frequency, any charges for obtaining the audits, as well as the rights to obtain the results of the audits in a timely manner. The contract may also specify rights to obtain documentation of the resolution of any deficiencies and to inspect the processing facilities and operating practices of the service provider. For Internet-related services, the contract should require periodic control reviews performed by an independent party with sufficient expertise. These reviews may include penetration testing, intrusion detection, reviews of firewall configuration, and other independent control reviews.

Managing Ongoing Monitoring

The due diligence is done, the contract is signed, and the service is being provided—but it's not yet time to relax. Remember that you can outsource the work but not the responsibility. Ongoing monitoring should include the effectiveness of the service providers' security controls, financial strength, ability to respond to changes in the regulatory environment, and the impact of external events. Business process owners should establish and maintain a professional relationship with key service provider personnel.

In Practice

Service Provider Management Policy

Synopsis: To establish the information security–related criteria for service provider relationships.

Policy Statement:

- *Service provider* is defined as a vendor, contractor, business partner, or affiliate who stores, processes, transmits, or accesses company information or company information systems.
- The Office of Risk Management is responsible for overseeing the selection, contract negotiations, and management of service providers.
- The Office of Risk Management will be responsible for conducting applicable service provider risk assessments.
- Due diligence research must be conducted on all service providers. Depending on risk assessment results, due diligence research may include but is not limited to:
  - Financial soundness review
  - Internal information security policy and control environment review
  - Review of any industry standard audit and/or testing of information security–related controls
- Service provider systems are required to meet or exceed internal security requirements. Safeguards must be commensurate with the classification of data and the level of inherent risk.
- Contracts and/or agreements with service providers will specifically require them to protect the CIA of all company, customer, and proprietary information that is under their control.
- Contracts and/or agreements must include notification requirements for suspected or actual compromise or system breach.
- Contracts and/or agreements must include the service provider's obligation to comply with all applicable state and federal regulations.
- As applicable, contracts and/or agreements must include a clause related to the proper destruction of records containing customer or proprietary information when no longer in use or if the relationship is terminated.
- Contracts and/or agreements must include provisions that allow for periodic security reviews/audits of the service provider environment.
- Contracts and/or agreements must include a provision requiring service providers to disclose the use of contractors.
- To the extent possible and practical, contractual performance will be monitored and/or verified. Oversight is the responsibility of the business process owner.

FYI: Small Business Note

The majority of small businesses do not have dedicated IT or information security staff. They rely on outside organizations or contractors to perform a wide range of tasks, including procurement, network management and administration, web design, and off-site hosting. Rarely are the "IT guys" properly vetted. A common small business owner remark is, "I wouldn't even know what to ask. I don't know anything about technology." Rather than being intimidated, small business owners and managers need to recognize that they have a responsibility to evaluate the credentials of everyone who has access to their information systems. Peer and industry groups such as the Chamber of Commerce, Rotary, ISC2, and ISACA chapters can all be a source for references and recommendations. As with any service provider, responsibilities and expectations should be codified in a contract.

Summary

This security domain is all about day-to-day operational activities. We started the chapter by looking at SOPs. We discussed that well-written SOPs provide direction, improve communication, reduce training time, and improve work consistency. Routine procedures that are short and require few decisions can be written using the simple step format. Long procedures consisting of more than ten steps, with few decisions, should be written in hierarchical steps format or in a graphic format. Procedures that require many decisions should be written in the form of a flowchart.

Organizations are dynamic, and change is inevitable. The objective of change control is to ensure that only authorized changes are made to software, hardware, network access privileges, or business processes. A change management process establishes an orderly and effective mechanism for submission, evaluation, approval, prioritization, scheduling, communication, implementation, monitoring, and organizational acceptance of change.

Two mandatory components of a change management process are an RFC (Request for Change) document and a change control plan. Scheduled changes can be exempt from the process as long as they have a preapproved procedure. A good example of this is patch management. A patch is software or code designed to fix a problem. Applying security patches is the primary method of fixing security vulnerabilities in software. Patch management is the process of scheduling, testing, approving, and applying security patches.

Criminals design malware, short for *malicious software* (or script or code), to exploit device, operating system, application, and user vulnerabilities with the intent of disrupting computer operations, gathering sensitive information, or gaining unauthorized access. A zero-day exploit is one that takes advantage of security vulnerability on the same day that the vulnerability becomes publicly or generally known. Malware categorization is based on infection and propagation characteristics. A virus is malicious code that attaches to and becomes part of another program. A worm is a piece of malicious code that can spread from one computer to another without requiring a host file to infect. A Trojan is malicious code that masquerades as a legitimate benign application. Bots (also known as robots) are snippets of code designed to automate tasks and respond to instructions. An entire network of compromised devices is known as a botnet. Ransomware is a type of malware that takes a computer or its data hostage in an effort to extort money from victims. A rootkit is set of software tools that hides its presence in the lower layers of the operating system application layer, operating system kernel, or in the device BIOS with privileged access permissions. Spyware is a general term used to describe software that, without a user's consent and/or knowledge, tracks Internet activity such as searches and web surfing, collects data on personal habits, and displays advertisements. Hybrid malware is code that combines characteristics of multiple categories. A blended threat is a when multiple variants of malware (worms, viruses, bots, and so on) are used in concert to exploit system vulnerabilities. An anti-malware defense-in-depth arsenal includes both prevention and detection controls. The most familiar of these is AV software that is designed to detect, contain, and in some cases eliminate malicious software.

Malware, user error, and system failure are among the many threats that can render data unusable. Having multiple copies of data is essential for both data integrity and availability. Data replication is the process of copying data to a second location that is available for immediate or near-time use. Data backup is the process of copying and storing data that can be restored to its original location. In both cases, it is essential to have SOPs for both replication/backup and restoration/recovery. Restoration and recovery processes should be tested to ensure that they work as anticipated.

Email is a primary malware distribution channel. Criminals embed malware in attachments or include a hyperlink to a malware distribution site. Email systems need to be configured to scan for malware and to filter attachments. Users need to be trained not to click email links and not to open unexpected attachments. Organizations should also restrict access to personal web mail applications because they bypass internal email controls. Criminals take advantage of the inherent weaknesses in the email communication system. The vulnerabilities can be traced back to the ARPANET, the precursor to the Internet, which was a US Advanced Research Project Agency (ARPA) project intended to develop a set of communications protocols to transparently connect computing resources in various geographical locations. Because the ARPANET was a trusted network, security controls were not considered. Today's email system uses essentially the same protocols and processes. Simple Mail Transfer Protocol (SMTP), designed in 1982, is the de facto message transport standard for sending email messages. Common mailbox access protocols Post Office Protocol (now POP3) and Internet Message Access Protocol (IMAP) were developed in 1984 and 1988, respectively. Messages sent using SMTP are transmitted in plaintext and are human readable. Multiple transport and storage encryption options can be used to protect the data from prying eyes. Encryption protects the privacy of the message by converting it from (readable) plaintext into (scrambled) cipher text. The default posture for many email servers is to process and relay any mail sent to the server; this feature is known as *open mail relay*. Criminals exploit open mail relay to distribute malware, spam, and illegal material such as pornography. A blacklist is a list of email addresses, domain names, or IP addresses known to be compromised or intentionally used as a distribution platform. The process of blacklisting is to use the blacklist as an email filter. Because email servers are Internet facing and are open to receiving packets, they are easy targets for distributed denial of service (DDoS) attacks. The objective of a DDoS attack is to render the service inoperable.

Almost every device and application on a network can record activity. This record of events is known as a log. Logs can be processed either using standard syslog protocols or using SIEM applications. Syslog provides an open framework based on message type and severity. Security information and event management software (SIEM) are commercial applications and often use proprietary processes. Analysis techniques include correlation, sequencing, signature comparison, and trend analysis. Correlation ties individual log entries together based on related information. Sequencing examines activity based on patterns. Signature compares log data to "known bad" activity. Trend analysis identifies activity over time that in isolation might appear normal. The process of configuring the log sources, including log generation, storage, and security, performing analysis of log data, initiating appropriate responses to identified events, and managing the long-term storage of log data is known as log management.

Operational security extends to service providers. Service providers are vendors, contractors, business partners, and affiliates who store, process, transmit, or access company information or company information systems. Service provider internal controls should meet or exceed those of the contracting organization. The conventional wisdom (and in some cases, the regulatory requirement) is that you can outsource the work but not the liability. Due diligence describes the process or methodology used to assess the adequacy of a service provider. SSAE16 audit reports have become the most widely accepted due diligence documentation. SSAE16 reports are independent audits certified by CPA firms. The three audit options are SOC 1, SOC 2, and SOC 3. SOC 1 audits focus on controls that are likely to be relevant to a service provider's financial statements and condition. SOC 2 and SOC 3 are designed to examine security, CIA, and privacy attributes. Once a vendor is selected, their obligations should be codified in a contract. Service provider contracts should include a number of information security–related clauses, including performance standards, security and privacy compliance requirements, incident notification, business continuity and disaster recovery commitments, and auditing and ongoing monitoring options.

Operations and Communications Security policies include Standard Operating Procedures Documentation Policy, Operational Change Control Policy, Security Patch Management Policy, Malicious Software Policy, Email and Email Systems Security Policy, Security Log Management Policy, and Service Provider Management Policy.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following is true about documenting SOPs?

   A. It promotes business continuity.

   B. The documentation should be approved before publication and distribution.

   C. Both A and B.

   D. Neither A nor B.

2. Which two factors influence the type of SOP used?

   A. Cost and complexity

   B. Number of decisions and number of steps

   C. Language and age of the workforce

   D. Number of warnings and number of exceptions

3. Which of the following formats should be used when an SOP includes multiple decision-making steps?

   A. Simple

   B. Hierarchical

   C. Graphic

   D. Flowchart

4. The change control process starts with which of the following?

   A. Budget

   B. RFC submission

   C. Vendor solicitation

   D. Supervisor authorization

5. What is the most important message to share with the workforce about "change"?

   A. The reason for the change

   B. The cost of the change

   C. Who approved the change

   D. Management's opinion of the change

6. Which of the following statements best describes the action that should occur prior to implementing a change that has the potential to impact business processing?

   A. The impact should be communicated.

   B. The change should be thoroughly tested.

   C. A rollback or recovery plan should be developed.

   D. All of the above.

7. Which of the following is *not* a part of a malware defense-in-depth strategy?

   A. Security awareness

   B. Prevention controls

   C. Reverse engineering

   D. Detection controls

8. Which of the following statements best describes a security patch?

   A. A security patch is designed to fix a security vulnerability.

   B. A security patch is designed to add security features.

   C. A security patch is designed to add security warnings.

   D. A security patch is designed to fix code functionality.

9. Which of the following is a component of an AV application?
   - A. Definition files
   - B. Handler
   - C. Patch
   - D. Virus

10. Which of the following statements best describes the testing of security patches?
    - A. Security patches should never be tested because waiting to deploy is dangerous.
    - B. Security patches should be tested prior to deployment, if possible.
    - C. Security patches should be tested one month after deployment.
    - D. Security patches should never be tested because they are tested by the vendor.

11. Which of the following operating systems are vulnerable to malware?
    - A. Apple OS only.
    - B. Android OS only.
    - C. Microsoft Windows OS only.
    - D. Malware is operating system agnostic.

12. Which of the following terms best describes malware that is specifically designed to hide in the background and gather info over an extended period of time?
    - A. Trojan
    - B. APT
    - C. Ransomware
    - D. Zero-day exploit

13. A __________________ can spread from one computer to another without requiring a host file to infect.
    - A. virus
    - B. Trojan
    - C. worm
    - D. rootkit

14. __________________ wait for remote instructions and are often used in DDoS attacks.
    - A. APTs
    - B. Bots
    - C. DATs
    - D. None of the above

15. Which of the following statements best describes a blended threat?

- **A.** A blended threat is designed to be difficult to detect.
- **B.** A blended threat is designed to be difficult to contain.
- **C.** A blended threat is designed to be difficult to eradicate.
- **D.** All of the above.

16. Which of the following statements best describes data replication?

- **A.** Replicated data needs to be restored from tape.
- **B.** Only administrators have access to replicated data.
- **C.** Replicated data is generally available in near or real time.
- **D.** Replication is expensive.

17. Organizations that are considering storing legally protected data in "the cloud" should ________________________.

- **A.** contractually obligate the service provider to protect the data
- **B.** assume that the appropriate security controls are in place
- **C.** give their customers an option as to where data is stored
- **D.** only use cloud storage for data replication

18. Which of the following actions best describes the task that should be completed once backup media such as tape is no longer in rotation?

- **A.** It should be erased and reused.
- **B.** It should be recycled.
- **C.** It should physically be destroyed.
- **D.** It should be labeled as old and put in a supply closet.

19. Which of the following terms best describes the Department of Defense project to develop a set of communications protocols to transparently connect computing resources in various geographical locations?

- **A.** DoDNet
- **B.** ARPANET
- **C.** EDUNET
- **D.** USANET

20. Which of the following terms best describes the message transport protocol used for sending email messages?

    A. SMTP
    B. SMNP
    C. POP3
    D. MIME

21. In its native form, email is transmitted in _________.

    A. cipher text
    B. clear text
    C. hypertext
    D. meta text

22. Which of the following statements best describes how users should be trained to manage their email?

    A. Users should click embedded email hyperlinks.
    B. Users should open unexpected email attachments.
    C. Users should access personal email from the office.
    D. Users should delete unsolicited or unrecognized emails.

23. Open email relay service can be used to do which of the following?

    A. Secure messages
    B. Ensure message delivery
    C. Misappropriate resources
    D. Create blacklists

24. Which of the following statements best describes a system log?

    A. A system log is a record of allowed and denied events.
    B. A system log is a record of problem events only.
    C. A system log is a record of user productivity.
    D. A system log is a record of system codes.

25. Which of the following statements best describes trend analysis?

    A. Trend analysis is used to tie individual log entries together based on related information.
    B. Trend analysis is used to examine activity based on patterns.
    C. Trend analysis is used to compare log data to known bad activity.
    D. Trend analysis is used to identify activity over time.

26. Which of the following statements best describes authentication server logs?

    A. Authentication server logs capture user, group, and administrative activity.
    B. Authentication server logs capture bad HTML code.
    C. Authentication server logs capture SQL injection attempts.
    D. Authentication server logs capture web traffic.

27. Which of the following terms best describes the process of assessing a service provider's reputation, financial statements, internal controls, and insurance coverage?

    A. Downstream investigation
    B. Standard of care
    C. Due diligence
    D. Outsource audit

28. SSAE16 audits must be attested to by a _____________.

    A. Certified Information System Auditor (CISA)
    B. Certified Public Accountant (CPA)
    C. Certified Information Systems Manager (CISM)
    D. Certified Information System Security Professional (CISSP)

29. Service providers should be required to provide notification of which of the following types of incidents?

    A. Confirmed incidents
    B. Confirmed incidents by known criminals
    C. Confirmed incidents that have been reported to law enforcement
    D. Confirmed and suspected incidents

30. Which of the following reasons best describes why independent security testing is recommended?

    A. Independent security testing is recommended because of the objectivity of the tester.
    B. Independent security testing is recommended because of the expertise of the tester.
    C. Independent security testing is recommended because of the experience of the tester.
    D. All of the above.

EXERCISES

EXERCISE 8.1: Documenting Operating Procedures

1. SOPs are not restricted to use in IT and information security. Cite three non-IT or security examples where SOP documentation is important.
2. Choose a procedure that you are familiar enough with that you can write SOP documentation.
3. Decide which format you are going to use to create the SOP document.

EXERCISE 8.2: Researching Email Security

1. Does your personal email application you are currently using have an option for "secure messaging"? If so, describe the option. If not, how does this limit what you can send via email?
2. Does the email application you are using have an option for "secure authentication" (this may be referred to as secure login or multifactor authentication)? If so, describe the option. If not, does this concern you?
3. Does the email application scan for malware or block attachments? If so, describe the option. If not, what can you do to minimize the risk of malware infection?

EXERCISE 8.3: Researching Metadata

1. Most applications include metadata in the document properties. What metadata does the word processing software you currently use track?
2. Is there a way to remove the metadata from the document?
3. Why would you want to remove metadata before distributing a document?

EXERCISE 8.4: Understanding Patch Management

1. Do you install operating system or application security patches on your personal devices such as laptops, tablets, and smartphone? If yes, how often. If not, why not?
2. What method do you use (for example, Windows Update)? Is the update automatic? What is the update schedule? If you do not install security patches, research and describe your options.
3. Why is it sometimes necessary to reboot your device after applying security patches?

EXERCISE 8.5: Understanding Malware Corporate Account Takeovers

1. Hundreds of small businesses across the country have been victims of corporate account takeovers. To learn more, read the following *NYT* small business article and visit the Krebs on Security blog. If the links are no longer active, Google the topic.

www.nytimes.com/2013/06/14/business/smallbusiness/protecting-business-accounts-from-hackers.html

https://krebsonsecurity.com/category/smallbizvictims

2. Should financial institutions be required to warn small business customers of the dangers associated with cash management services such as ACH and wire transfers? Explain your reasoning.

3. What would be the most effective method of teaching bank customers about corporate account takeover attacks?

PROJECTS

PROJECT 8.1: Performing Due Diligence with Data Replication and Backup Service Providers

1. Do you store your schoolwork on your laptop? If not, where is the data stored? Write a memo explaining the consequences of losing your laptop, or if the alternate location or device becomes unavailable. Include the reasons why having a second copy will contribute to your success as a student. After you have finished step 2 of this project, complete the memo with your recommendations.

2. Research "cloud-based" backup or replication options. Choose a service provider and answer the following questions:

   What service/service provider did you choose?

   How do you know they are reputable?

   What controls do they have in place to protect your data?

   Do they reveal where the data will be stored?

   Do they have an SSAE16 or equivalent audit report available for review?

   Do they have any certifications, such as McAfee Secure?

   How much will it cost?

   How often are you going to update the secondary copy?

   What do you need to do to test the restore/recovery process?

   How often will you test the restore/recovery process?

PROJECT 8.2: Developing an Email and Malware Training Program

You are working as an information security intern for Best Regional Bank, who has asked you to develop a PowerPoint training module that explains the risks (including malware) associated with email. The target audience is all employees.

1. Create an outline of the training to present to the training manager.
2. The training manager likes your outline. She just learned that the company would be monitoring email to make sure that data classified as "protected" is not being sent insecurely and that access to personal web-based email is going to be restricted. You need to add these topics to your outline.
3. Working from your outline, develop a PowerPoint training module. Be sure to include email "best practices." Be prepared to present the training to your peers.

PROJECT 8.3: Developing Change Control and SOPs

The Dean of Academics at ABC University has asked your class to design a change control process specifically for mid-semester faculty requests to modify the day, the time, or the location where their class meets. You need to do the following:

1. Create an RFC form.
2. Develop an authorization workflow that specifies who (for example, the department chair) needs to approve the change and in what order.
3. Develop an SOP flowchart for faculty members to use that includes submitting the RFC, authorization workflow, and communication (for example, students, housekeeping, campus security, registrar).

Case Study

Using Log Data to Identify Indicators of Compromise

Log data offer clues about activities that have unexpected—and possibly harmful—consequences. The following parsed and normalized firewall log entries indicate a possible malware infection and data exfiltration. The entries show a workstation making connections to Internet address 93.177.168.141 and receiving and sending data over TCP port 16115.

```
id=firewall sn=xxxxxxxxxxxx time="2013-04-02 11:53:12 UTC" fw=255.255.255.1 pri=6
  c=262144
m=98 msg="Connection Opened" n=404916 src=10.1.1.1 (workstation) :49427:X0
dst=93.177.168.141 :16115:X1 proto=tcp/16115
id=firewall sn=xxxxxxxxxxxx time="2013-04-02 11:53:29 UTC" fw=255.255.255.1 pri=6
  c=1024
m=537 msg="Connection Closed" n=539640 src=10.1.1.1 (workstation) :49427:X0
dst=93.177.168.141 :16115:X1 proto=tcp/16115 sent=735 rcvd=442
```

```
id=firewall sn=xxxxxxxxxxxx time="2013-04-02 11:53:42 UTC" fw=255.255.255.1 pri=6
  c=262144
m=98 msg="Connection Opened" n=404949 src=10.1.1.1 (workstation) :49430:X0
dst=93.177.168.141 :16115:X1 proto=tcp/16115
id=firewall sn=xxxxxxxxxxxx time="2013-04-02 11:54:30 UTC" fw=255.255.255.1 pri=6
  c=1024
m=537 msg="Connection Closed" n=539720 src=10.1.1.1 (workstation) :49430:X0
dst=93.177.168.141 :16115:X1 proto=tcp/16115 sent=9925 rcvd=639
```

1. Describe what is happening.
2. Is the log information useful? Why or why not?
3. Research the destination IP address (dst) and the protocol/port (proto) used for communication.
4. Can you find any information that substantiates a malware infection and data exfiltration?
5. What would you recommend as next steps?

References

Regulations Cited

"16 CFR Part 314: Standards for Safeguarding Customer Information; Final Rule, Federal Register," accessed on 05/2013, http://ithandbook.ffiec.gov/media/resources/3337/joisafeguard_customer_info_final_rule.pdf.

"Federal Information Security Management Act (FISMA)," accessed on 06/2013, http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

"Gramm-Leach-Bliley Act," the official website of the Federal Trade Commission, Bureau of Consumer Protection Business Center, accessed on 05/2013, http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

"HIPAA Security Rule," the official website of the Department of Health and Human Services, accessed on 05/2013, www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

Other References

Ducklin, Paul. "Memories of Slammer—Ten Years Later," January 27, 2013, Sophos Naked Security, accessed 07/2013, http://nakedsecurity.sophos.com/2013/01/27/memories-of-the-slammer-worm/.

"Enterprise Blended Malware Threats Slip through Traditional Defenses," Blue Ridge Networks, Inc., whitepaper, March 16, 2012, accessed 07/2013, www.blueridge.com/support/downloads/Enterprise%20Blended%20Malware%20Threat%20WP%20v2.pdf.

FFIEC Information Security IT Examination Handbook, accessed 07/2013, www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf.

FFEIC Information Audit IT Examination Handbook, accessed 07/2013, www.ffiec.gov/ffiecinfobase/booklets/audit/audit.pdf.

"Infographic: The State of Malware 2013," April 1, 2013, accessed 07/2013, www.mcafee.com/us/security-awareness/articles/state-of-malware-2013.aspx.

"ISO 5807:1985," ISO, accessed 07/2013, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=11955.

Kern, Harris. "How to Implement Change Management with These Six Steps," Yahoo! Voices, May 25, 2009, accessed 07/2013, http://voices.yahoo.com/how-implement-change-management-these-six-3388866.html.

"Management Best Practices Benchmarking Report," Change Management Learning Center, accessed 07/2013, www.change-management.com/tutorial-communications.htm.

NSA Sixty-Minute Security Guide, accessed 07/2013, www.nsa.gov/snac/support/I33-011R-2006.pdf.

NIST Special Publication 800-42: Guideline on Network Security Testing, accessed 07/2013, http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.

"Project Documentation Guidelines, Virginia Tech," accessed 07/2013, www.itplanning.org.vt.edu/pm/documentation.html.

"Service Organization Controls, Managing Risks by Obtaining a Service Auditors Report," February 2013, American Institute of CPAs, accessed 2013, www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx.

Skoudis, Ed. *Malware: Fighting Malicious Code*, Prentice Hall, 2003.

Still, Michael and Eric Charles McCreath. "DDoS Protections for SMTP Servers." *International Journal of Computer Science and Security*, Volume 4, Issue 6, 2011.

"What Is Ransomware?" Microsoft Protection Center, accessed 07/2013, www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx.

"What Is Spyware," Microsoft Safety & Security Center, accessed 07/2013, www.microsoft.com/security/pc-security/spyware-whatis.aspx.

"What Is the Difference: Viruses, Worms, Trojans, and Bots," accessed 07/2013, www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html.

Wieringa, Douglas, Christopher Moore, and Valerie Barnes. *Procedure Writing: Principles and Practices, Second Edition*, Columbus, Ohio: Battelle Press, 1988.

This page intentionally left blank

Chapter 9

Access Control Management

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Explain access control fundamentals.
- Apply the concepts of default deny, need-to-know, and least privilege.
- Understand secure authentication.
- Protect systems from risks associated with Internet connectivity, remote access, and telework environments.
- Manage and monitor user and administrator access.
- Develop policies to support access control management.

What could be more essential to security than managing access to information and information systems? The primary objective of access controls is to protect information and information systems from unauthorized access (confidentiality), modification (integrity), or disruption (availability). The access control management domain incorporates the most fundamental precepts in information security: deny all, least privilege, and need-to-know.

We will begin this chapter with a broad discussion of access control concepts and security models with a focus on authentication and authorization. We will examine the factors of authentication with an emphasis on the importance of multifactor authentication. We will look at the mandatory and discretionary authorization options for granting access rights and permission. We will consider the risks associated with administrative and privileged accounts. Reaching past the boundaries of the internal network, we will apply these concepts to the infrastructure, including border security, Internet access, remote access, and the teleworking environment. We will be mindful of the need to audit and monitor entry and exit points and to be prepared to respond to security violations. Throughout the chapter, we will develop policies designed to support user access and productivity while simultaneously mitigating the risk of unauthorized access.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 9 of ISO 27002:2013 is dedicated to access control, with the objective of managing authorized access and preventing unauthorized access to information systems. This domain extends to remote locations, home offices, and mobile access.

Corresponding NIST guidance is provided in the following documents:

- SP 800-94: Guide to Intrusion Detection and Prevention Systems
- SP 800-41, R1: Guidelines on Firewalls and Firewall Policy
- SP 800-46, R1: Guide to Enterprise Telework and Remote Access Security
- SP 800-77: Guide to IPsec VPNs
- SP 800-114: User's Guide to Securing External Devices for Telework and Remote Access
- SP 800-113: Guide to SSL VPNs
- SP 800-225: Guidelines for Securing Wireless Local Area Networks (WLANs)

Access Control Fundamentals

Access controls are security features that govern how users and processes communicate and interact with systems and resources. The primary objective of access controls is to protect information and information systems from unauthorized access (confidentiality), modification (integrity), or disruption (availability). When we're discussing access controls, the active entity (that is, the user or system) that requests access to a resource or data is referred to as the ***subject*** and the passive entity being accessed or being acted upon is referred to as the ***object***.

An identification scheme, an authentication method, and an authorization model are the three common attributes of all access controls. An ***identification scheme*** is used to identify unique records in a set, such as a user name. ***Identification*** is the process of the subject supplying an identifier to the object. The ***authentication method*** is how identification is proven to be genuine. ***Authentication*** is the process of the subject supplying verifiable credentials to the object. The ***authorization model*** defines how access rights and permission are granted. ***Authorization*** is the process of assigning authenticated subjects the permission to carry out a specific operation.

The security posture of an organization determines the default settings for access controls. Access controls can be technical (such as firewalls or passwords), administrative (such as separation of duties or dual controls), or physical (such as locks, bollards, or turnstiles).

What Is a Security Posture?

A ***security posture*** is an organization's approach to access controls. The two fundamental postures are open and secure. ***Open***, also referred to as ***default allow***, means that access, not explicitly forbidden, is permitted. ***Secure***, also referred to as ***default deny***, means that access, not explicitly permitted, is forbidden. In practical application, ***default deny*** means that access is unavailable until a rule, access control list (ACL), or setting is modified to allow access.

The challenge for organizations that adopt a secure posture is that a number of devices on the market today, including tablets and smartphones as well as software applications, come with an out-of -the-box setting of default allow. Why? Interoperability, ease of use, and productively are the three reasons cited. The explosive growth in the use of technology, coupled with increasing awareness of vulnerabilities, is creating a shift in the industry. Organizations have become more security conscious and are beginning to demand more secure products from their vendors. Microsoft is an example of a company that has responded to market requirements. Early Windows server operating systems were configured as default allow. Current Windows server operating systems are configured as default deny.

Need-to-Know and Least Privilege

Determining who to grant access to should be based on the security principle of need-to-know. The level of access required should be based on the security principle of least privilege. Need-to-know means that the subject has a demonstrated and authorized reason for being granted access to information. Once a need-to-know has been established, ***least privilege*** is the principle of only assigning required object access permissions. Applied to the workforce, the principle of least privilege means granting users the least amount of access required to perform their job and no more. For example, if a user only needs to read a document, then only the "read" right is granted. If a user needs to be able to edit a document, then the "read" and "modify" permissions would be granted. The objective of both principles is to limit the potential damage of a security breach, whether accidental or malicious.

How Is Identity Verified?

Granting access is a multistep process that begins with the positive identification of the person or process seeking access to a system or resource. The process of ***authentication*** requires the subject to supply verifiable credentials. The credentials are often referred to as ***factors***. There are three categories of factors: knowledge (something the user knows), possession (something a user has), and inherence (something the user is). ***Single-factor authentication*** is when only one factor is presented. The most common method of single-factor authentication is the password. ***Multifactor authentication*** is when two or more factors are presented. ***Multilayer authentication*** is when two or more of the same type of factors are presented. Data classification, regulatory requirements, the impact of unauthorized access, and the likelihood of a threat being exercised should all be considered when you're deciding on the level of authentication required. The more factors, the more robust the authentication process.

Knowledge: Something You Know

Something you know is knowledge-based authentication. It could be a string of characters, referred to as a password or PIN, or it could be an answer to a question. Passwords are the most commonly used single-factor network authentication method. The authentication strength of a password is a function of its length, complexity, and unpredictability. If it is easy to guess or deconstruct, it is vulnerable to attack. Once known, it is no longer useful as a verification tool. The challenge is to get users to create, keep secret, and remember secure passwords. Weak passwords can be discovered within minutes or even seconds using any number of publicly available password crackers or social engineering techniques. Best practices dictate that passwords are a minimum of eight characters in length (preferably longer), include a combination of at least three upper and/or lowercase letters, punctuation, symbols, and numerals (referred to as complexity), are changed frequently, and are unique. Using the same password to log in to multiple applications and sites significantly increases the risk of exposure.

Generally, when users are granted initial access to an information system, they are given a temporary password. Most systems have a technical control that will force the user to change his or her password at first login. Passwords should be changed immediately if there is any suspicion that it has been compromised.

As any help desk person will tell you, users forget their passwords with amazing regularity. If a user forgets his password, there needs to be a process for reissuing passwords that includes verification that the requester is indeed who he says he is. Often cognitive passwords are used as secondary verification. A ***cognitive password*** is a form of knowledge-based authentication that requires a user to answer a question based on something familiar to them. Common examples are mother's maiden name and favorite color. The problem, of course, is that this information is very often publicly available. This weakness can be addressed using sophisticated questions that are derived from subscription databases such as credit reports. These questions are commonly referred to as ***out-of-wallet*** challenge questions. The term was coined to indicate that the answers are not easily available to someone other than the user, and that the user is not likely to carry such information in his or her wallet. Out-of-wallet question systems usually require that the user correctly answer more than one question and often include a "red herring" question that is designed to trick an imposter but which the legitimate user will recognize as nonsensical.

It may seem very convenient when a website or application offers to remember a user's log on credentials or provide an automatic logon to a system, but this practice should be strictly prohibited. If a user allows websites or software applications to automate the authentication process, then unattended devices can be used by unauthorized people to gain access to information resources.

FYI: Yahoo! Password Compromise

Do these passwords look familiar to you? In July of 2012, the hacker group D33ds Company claimed responsibility for attacking Yahoo! Voice and exposing 453,492 plain text login credentials. The full data dump was made available on Pastebin. The top ten most used passwords in order of popularity are listed here. Additional information is available at http://pastebin.com/2D6bHGTa.

1. 123456 (38%)
2. password (18%)
3. welcome (10%)
4. ninja (8%)
5. abc123 (6%)
6. 123456789 (5%)
7. 12345678 (5%)
8. sunshine (5%)
9. princess (5%)
10. qwerty (4%)

Possession: Something You Have

The second factor of authentication requires that the subject be in physical possession of a unique identifier. Examples include a one-time passcode, memory cards, smartcard, and out-of-band communication. The most common of the four is the one-time passcode sent to a device in the user's possession. A ***one-time passcode (OTP)*** is a set of characteristics that can be used to prove a subject's identity one time and one time only. Because the OTP is only valid for one access, if captured, additional access would be automatically denied. OTPs are generally delivered through a hardware or software token device. The token displays the code, which must then be typed in at the authentication screen. Alternatively, the OTP may be delivered via email, text message, or phone call to a predetermined address or phone number.

A ***memory card*** is an authentication mechanism that holds user information within a magnetic strip and relies on a reader to process the information. The user inserts the card into the reader and enters a personal identification number (PIN). Generally, the PIN is hashed and stored on the magnetic strip. The reader hashes the inputted PIN and compares it to the value on the card itself. A familiar example of this is a bank ATM card. A ***smartcard*** works in a similar fashion. Instead of a magnetic strip, it has a microprocessor and integrated circuits. The user inserts the card into a reader, which has electrical contacts that interface with the card and power the processor. The user enters a PIN that "unlocks" the information. The card can hold the user's private key, generate an OTP, or respond to a challenge-response.

Out-of-band authentication requires communication over a channel that is distinct from the first factor. A cellular network is commonly used for out-of-band authentication. For example, a user enters her name and password at an application logon prompt (factor 1). The user then receives a call on her mobile phone; the user answers and provides a predetermined code (factor 2). In order for the authentication to be compromised, the attacker would have to have access to both the computer and the phone.

FYI: Google 2-Step Verification

In response to password insecurity, in 2011, Google launched an optional 2-step verification process. With 2-step verification, accounts are protected by something you know (password) and something you have (one-time verification code provided to you). Google offers a variety of ways to get the code, including text message, phone call, Google authenticator app for Android, iPhone, and Blackberry, and a printable list of one-time codes. According to Google, as of July 2013, millions of users have made their accounts stronger with 2-step verification. Have you?

Inherence: Something You Are

The third factor of authentication is you. ***Biometrics*** is the identification of humans by distinctive, measurable characteristics or traits. A biometric identification system scans an attribute of a person and compares it to a record that was created in an earlier enrollment process. Success of the system depends on accurate and repeatable measurements of anatomical or physiological attributes.

Anatomical attributes include fingerprint, finger scan, palm scan, hand geometry, retina scan, iris scan, facial scan, and DNA. Physiological attributes includes handwriting, keyboard dynamics, and voice print. Biometric authentication is the most accurate factor; it is also the most expensive to implement and maintain.

In Practice

Authentication Policy

Synopsis: To require the positive identification of the person or system seeking access to secured information, information systems, or devices.

Policy Statement:

- Access to and use of information technology (IT) systems must require an individual to uniquely identify and authenticate him/herself to the resource.
- Multiuser or shared accounts are allowed only when there is a documented and justified reason that has been approved by the Office of Information Security.
- The Office of Information Security is responsible for managing an annual user account audit of network accounts, local application accounts, and web application accounts.
- Data classification, regulatory requirements, the impact of unauthorized access, and the likelihood of a threat being exercised must all be considered when deciding upon the level of authentication required. The Office of Information Security will make this determination in conjunction with the information system owner.
- Operating systems and applications will at a minimum be configured to require single-factor complex password authentication:

  - The inability to technically enforce this standard does not negate the requirement.
  - Password length, complexity, and expiration will be defined in the company password standard.
  - The password standard will be published, distributed, and included in the acceptable use agreement.
- Web applications that transmit, store, or process “protected” or “confidential” information must at a minimum be configured to require single-factor complex password authentication:
  - The inability to technically enforce this standard does not negate the requirement.
  - Password length, complexity, and expiration will be defined in the company password standard.
  - If available, multifactor authentication must be implemented.
  - Passwords and PINs must be unique to the application.
  - Exceptions to this policy must be approved by the Office of Information Security.
- All passwords must be encrypted during transmission and storage. Applications that do not conform to this requirement may not be used.
- Any mechanism used for storing passwords must be approved by the Office of Information Security.
- If any authentication mechanism has been compromised or is suspected of being compromised, users must immediately contact the Office of Information Security and follow the instructions given.

What Is Authorization?

Once authenticated, a subject must be authorized. ***Authorization*** is the process of assigning authenticated subjects permission to carry out a specific operation. The ***authorization model*** defines how access rights and permission are granted. The three primary authorization models are object capability, security labels, and ACLs. ***Object capability*** is used programmatically and is based on a combination of an unforgeable reference and an operational message. ***Security labels*** are mandatory access controls embedded in object and subject properties. ***Access control lists (ACLs)*** are used to determine access based on some combination of specific criteria, such as a user ID, group membership, classification, location, address, and date. The three categories of ACLs are discretionary access controls, role-based access controls, and rule-based access controls.

Mandatory Access Control (MAC)

Mandatory access controls (MACs) are defined by policy and cannot be modified by information owner. MACs are primarily used in secure military and government systems that require a high degree of confidentiality. In a MAC environment, objects are assigned a security label that indicates the classification and category of the resource. Subjects are assigned a security label that indicates a clearance level and assigned categories (based on need-to-know). The operating system compares the object’s security label with the subject's security label. The subject's clearance must be equal to or greater than the object's classification. The category must match. For example, in order for a user to access a document classified as "Secret" and categorized as "Flight Plans," the user must have either Secret or Top Secret clearance and have been tagged to the Flight Plan category.

Discretionary Access Control (DAC)

Discretionary access controls (DACs) are defined by the owner of the object. DACs are used in commercial operating systems. The object owner builds an ACL that allows or denies access to the object based on the user's unique identity. The ACL can reference a user ID or a group (or groups) that the user is a member of. Permissions can be cumulative. For example, John belongs to the Accounting Group. The Accounting Group is assigned read permissions to the Income Tax folder and the files in the folder. John's user account is assigned write permissions to the Income Tax folder and the files in the folder. Because DAC permissions are cumulative, John can access, read, and write to the files in the tax folder.

Role-Based Access Control (RBAC)

Role-based access controls (RBACs) (also called non-discretionary) are access permissions based on a specific role or function. Administrators grant access rights and permissions to roles. Users are then associated with a single role. There is no provision for assigning rights to a user or group account. For example, Sally is associated with the role of "Programmer." Sally will inherit all of the permissions assigned to the Programmer role. Sally cannot be assigned any additional permissions.

Rule-based Access Control

In a ***rule-based access controls*** environment, access is based on criteria that is independent of the user or group account. The rules are determined by the resource owner. Commonly used criteria include source or destination address, geographic location, and time of day. For example, the ACL on an application requires that it be accessed from a specific workstation. Rule-based access controls can be combined with DACs and RBACs.

In Practice

Access Control Authorization Policy

Synopsis: To state the access control authorization principles of the organization.

Policy Statement:

- Default access privileges will be set to "deny all."
- Access to information and information systems must be limited to personnel and processes with a need-to-know to effectively fulfill their duties.

- Access permissions must be based on the minimum required to perform the job or program function.
- Information and information system owners are responsible for determining access rights and permissions.
- The Office of Information Security is responsible for enforcing an authorization process.
- Permissions must not be granted until the authorization process is complete.

Infrastructure Access Controls

A ***network infrastructure*** is defined as an interconnected group of hosts and devices. The infrastructure can be confined to one location or, as often is the case, widely distributed, including branch locations and home offices. Access to the infrastructure enables the use of its resources. ***Infrastructure access controls*** include physical and logical network design, border devices, communication mechanisms, and host security settings. Because no system is foolproof, access must be continually monitored; if suspicious activity is detected, a response must be initiated.

Why Segment a Network?

Network segmentation is the process of logically grouping network assets, resources, and applications. Segmentation provides the flexibility to implement a variety of services, authentication requirements, and security controls. Working from the inside out, network segments include the following types:

- **Enclave network**—A segment of an internal network that requires a higher degree of protection. Internal accessibility is further restricted through the use of firewalls, VPNs, VLANs, and network access control (NAC) devices.
- **Trusted network (wired or wireless)**—The internal network that is accessible to authorized users. External accessibility is restricted through the use of firewalls, VPNs, and IDS/IPS devices. Internal accessibility may be restricted through the use of VLANs and NAC devices.
- **Semi-trusted network, perimeter network, or DMZ**—A network that is designed to be Internet accessible. Hosts such as web servers and email gateways are generally located in the DMZ. Internal and external accessibility is restricted through the use of firewalls, VPNs, and IDS/IPS devices.
- **Guest network (wired or wireless)**—A network that is specifically designed for use by visitors to connect to the Internet. There is no access from the Guest network to the internal trusted network.
- **Untrusted network**—A network outside your security controls. The Internet is an untrusted network.

Introduced commercially in 1980, Ethernet is the most widely used wired local area network (LAN) technology. The components are mature and the security issues well understood. In contrast, wireless local area network (WLAN) technologies and corresponding security standards for exchanging data through radio communications are emerging. NIST SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs) provides recommendations for WLAN security configuration, including configuration design, implementation, evaluation, maintenance, and monitoring.

In Practice

Network Segmentation Policy

Synopsis: Directive to logically group network assets, resources, and applications for the purpose of applying security controls.

Policy Statement:

- The network infrastructure will be segregated into distinct segments according to security requirements and service function.
- The Office of Information Security and the Office of Information Technology are jointly responsible for conducting annual network segment risk assessments. The results of the assessments will be provided to the Chief Operating Officer (COO).
- Complete documentation of the network topology and architecture will be maintained by the Office of Information Technology, including an up-to-date network diagram showing all internal (wired and wireless) connections, external connections, and end points, including the Internet.

What Is Layered Border Security?

Layered security is the term applied to having different types of security measures designed to work in tandem with a single focus. The focus of ***layered border security*** is protecting the internal network from external threats. Layered border security access controls include firewall devices, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs). In order to be effective, these devices must be properly configured and expertly managed. Due to the complexity of and resource requirements associated with maintaining and monitoring border security devices, many organizations have chosen to outsource the function to ***managed security service providers*** (referred to as MSSPs). Oversight of in-house administration or of the MSSP is a critical risk management safeguard.

Firewalls

Firewalls are devices or software that control the flow of traffic between networks. They are responsible for examining network entry and exit requests and enforcing organizational policy. Firewalls are a mandatory security control for any network connected to an untrusted network such as the Internet. Without a properly configured firewall, a network is completely exposed and could potentially be compromised within minutes, if not seconds. A firewall policy defines how the firewall should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, ports, applications, and content types. The policy is codified in the rule set. The rule set is used by the firewall to evaluate ***ingress*** (incoming) and ***egress*** (outgoing) network traffic. In keeping with access control best practices, rule sets should be initially set to “deny all” and then strict rules implemented that allow connectivity based on business need.

NIST SP-41, R1: Guidelines on Firewalls and Firewall Policy provides an overview of firewall technologies and discusses their security capabilities and relative advantages and disadvantages in detail. It also provides examples of where firewalls can be placed within networks, and the implications of deploying firewalls in particular locations. The document also makes recommendations for establishing firewall policies and for selecting, configuring, testing, deploying, and managing firewall solutions.

FYI: IP Address, Ports, and Protocols Simplified

IP addresses, ports, and protocols form the basis of Internet communications:

- An ***IP address*** is how a specific network host or device is identified.
- A ***port*** is how an application or service is identified.
- A ***protocol*** is a standardized way for hosts and network devices to exchange information.

Let’s compare IP addresses, ports, and protocols to mailing a letter.

If you want to mail a letter, you must follow the postal protocol, including how to address the letter to the recipient, the return address requirements, and where a letter can be mailed (such as the post office or mailbox).

The address must include the city (network), the street (network segment), and house number (host or device).

In order to be delivered to the right person (application or service), the address must include a unique name (port).

Intrusion Detection Systems and Intrusion Protection Systems

It is possible for malicious activity to masquerade as legitimate traffic. ***Intrusion detection systems (IDSs)*** are passive devices designed to analyze network traffic in order to detect unauthorized access or malevolent activity. Most IDSs use multiple methods to detect threats, including signature-based detection, anomaly-based detection, and stateful protocol analysis. If suspicious activity is detected, IDSs generate an onscreen, email, and/or text alert. ***Intrusion prevention systems (IPSs)*** are active devices that sit inline with traffic flow and can respond to identified threats by disabling the connection, dropping the packet, or deleting the malicious content.

There are four types of IDS/IPS technologies:

- **Network-based IDS/IPS**—Monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity

- **Wireless IDS/IPS**—Monitors wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves
- **Network behavior analysis IDS/IPS**—Examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (for example, a client system providing network services to other systems)
- **Host-based IDS/IPS**—Monitors the characteristics of a single host and the events occurring within that host for suspicious activity

IDS/IPS has four decision states. ***True positive*** occurs when the IDS/IPS correctly identifies an issue. ***True negative*** occurs when the IDS/IPS correctly identifies normal traffic. ***False positive*** occurs when the IDS/IPS incorrectly identifies normal activity as an issue. ***False negative*** occurs when the IDS/ISP incorrectly identifies an issue as normal activity.

NIST SP-94: Guide to Intrusion Detection and Prevention Systems describes the characteristics of IDS and IPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them. The types of IDS/IPS technologies are differentiated primarily by the types of events they monitor and the ways in which they are deployed.

Content Filtering and Whitelisting/Blacklisting

Controls are required to protect the internal network from insider requests that could result in malware distribution, data exfiltration, participation in peer-to-peer (P2P) networks, and viewing of inappropriate or illegal content. The insider request could come from authenticated authorized users or could be a response to a malicious command or instruction. As discussed earlier, border device egress filters can and should be used to restrict outbound traffic by source and destination address, port, and protocol. The filters can be supplemented by self-generated, open source, or subscription-based IP whitelists and/or blacklists. ***Whitelists*** are addresses (IP and/or Internet domain names) of known "good" sites to which access should be allowed. Conversely, ***blacklists*** are addresses (IP and/or Internet domain names) of known "bad" sites to which access should be denied. It is common practice to block entire ranges of IP addresses specific to geographic regions. ***Content-filtering*** applications can be used to restrict access by content category (such as violence, gaming, shopping, or pornography), time factors, application type, bandwidth use, and media.

Border Device Administration and Management

Border device administration and management is a 24/7/365 responsibility. On a daily basis, performance needs to be monitored to enable potential resource issues to be identified and addressed before components become overwhelmed. Logs and alerts must be monitored and analyzed to identify threats—both successful and unsuccessful. Administrators need to be on the watch for security patches and apply them expediently. Border device policies, configurations, and rule sets must be backed up or replicated.

Policy rules and rule sets need to be updated as the organization's requirements change or when new threats are identified. Changes should be closely monitored because unauthorized or incorrect modifications to the rule set can put the organization at risk. Modifications should be subject to the organization's change management process. This includes a separation of approval and implementation duties. Configuration and rule set reviews as well as testing should be performed periodically to ensure continued compliance with the organization's policies. Internal reviews can uncover configuration settings and rules that are outdated, redundant, or harmful. The review should include a detailed examination of all changes since the last regular review, particularly who made the changes and under what circumstances. External penetration testing can be used to verify that the devices are performing as intended.

FYI: Blue Versus Red Team Penetration Test

The two approaches to conducting penetration testing are Blue Teaming and Red Teaming. A penetration test performed with the knowledge and consent of the organization's IT staff is known as ***Blue Teaming***, which is generally conducted to identify device or application vulnerabilities. A penetration test conducted without the knowledge of the organization's IT staff but with full knowledge and permission of the upper management is known as ***Red Teaming***. The objective of Red Teaming is to identify vulnerabilities as well as an organization's attack detection and response capabilities.

In Practice

Border Device Security Access Control Policy

Synopsis: Requirements for the secure design, configuration, management, administration, and oversight of border devices.

Policy Statement:

- Border security access control devices will be implemented and securely maintained to restrict access between networks that are trusted to varying degrees.
- The default policy for handling inbound and outbound traffic should be to deny all.
- If any situation renders the Internet-facing border security devices inoperable, Internet service must be disabled.
- The Office of Information Security is responsible for approving border security access control architecture, configuration, and rule sets.
- The Office of Information Technology is responsible for designing, maintaining, and managing border security access control devices:
  - At the discretion of the COO, this function or part of it may be outsourced to an MSSP.
  - Oversight of internal or MSSP border security device administrators is assigned to Office of Information Security.

- The types of network traffic that must always be denied without exception will be documented in the border device security standards.
- Rule sets must be as specific and simple as possible. Rule set documentation will include the business justification for allowed traffic.
- All configuration and rule set changes are subject to the organizational change management process.
  - All rule set modifications must be approved by the Office of Information Security.
- All border security access control devices must be physically located in a controlled environment, with access limited to authorized personnel.
- To support recovery after failure or natural disaster, the border security device configuration, policy, and rules must be backed up or replicated on a scheduled basis as well as before and after every configuration change.
- Border devices must be configured to log successful and failed activity as well as configuration changes.
- Border device logs must be reviewed daily by the Office of Information Technology or MSSP, and an activity report must be submitted to the Office of Information Security.
- Configuration and rule set reviews must be conducted annually:
  - The review is to be conducted by an external, independent entity.
  - Selection of the vendor is the responsibility of the Audit Committee.
  - Testing results are to be submitted to the COO.
- External penetration testing must, at a minimum, be performed semi-annually:
  - The testing is to be conducted by an external, independent entity.
  - Selection of the vendor is the responsibility of the Audit Committee.
  - Testing results are to be submitted to the COO.

Remote Access Security

The need to access internal corporate network resources from external locations has become increasingly common. Matter of fact, for companies with a remote or mobile workforce, remote access has become the norm. The nature of remote access technologies—permitting access to protected resources from external networks and often external hosts as well—is fraught with risk. Companies should start with the assumption that external facilities, networks, and devices contain hostile threats that will, if given the opportunity, attempt to gain access to the organization’s data and resources. Controls, including authentication, must be carefully evaluated and chosen based on the network segment’s information systems and the classification of information that will be accessible. Consideration must be given to ensuring that the remote access communication and stored user data cannot be accessed or read by unauthorized parties (confidentiality), detecting intentional or unintentional modifications to data in transit (integrity), and ensuring that users can access the resources as required (availability). Remote access security controls that must be considered include the physical security of the client devices, use of cryptography in transit, the method of authentication and authorization, and the risks associated with local storage.

NIST SP 800-46, R1: Guide to Enterprise Telework and Remote Access Security provides information on security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework and remote access technologies. The publication also provides recommendations for creating telework-related policies and for selecting, implementing, and maintaining the necessary security controls for remote access servers and clients.

Remote Access Technologies

The two most common remote access technologies are virtual private networks (VPNs) and remote access portals. VPNs are generally used to extend the resources of a network to a remote location. Portals are generally used to provide access to specific applications.

A ***virtual private network (VPN)*** provides a secure tunnel for transmitting data through an unsecured network such as the Internet. This is achieved using tunneling and encryption in combination to provide high security remote access without the high cost of dedicated private lines. ***IPsec*** (short for IP Security) is a set of protocols developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets at the IP layer. IPsec is most commonly associated with VPNs as the protocol providing tunneling and encryption for VPN connections between physical sites or between a site and a remote user. The tunnel can be thought of as a virtual pathway between systems within the larger pathway of the Internet. The popularity of VPN deployments is a result of worldwide low-cost accessibility to the Internet, in contrast to private circuits that are expensive, require long-term contracts, and must be implemented between specific locations. More information on IPsec VPNs is available from NIST SP 800-77: Guide to IPsec VPNs, and more information on SSL tunnel VPNs is available from NIST SP 800-113: Guide to SSL VPNs.

A ***remote access portal*** offers access to one or more applications through a single centralized interface. A portal server transfers data to the client device as rendered desktop screen images or web pages, but data is typically stored on the client device temporarily. Portals limit remote access to specific portal-based applications. Another type of portal solution is terminal server access, which gives each remote user access to a separate standardized virtual desktop. The terminal server simulates the look and feel of a desktop operating system and provides access to applications. Terminal server access requires the remote user either to install a special terminal server client application or to use a web-based interface, often with a browser plug-in or other additional software provided by the organization. What's more, applications such as Teamview and Joinme are specifically designed to create remote desktop sessions.

Remote Access Authentication and Authorization

Whenever feasible, organizations should implement ***mutual authentication*** so that a remote access user can verify the legitimacy of a remote access server before providing authentication credentials to it. The presentation of a preselected picture is an example of server-side authentication. Best practices dictate that multifactor authentication be required for remote access authentication. In order for an attacker to gain unauthorized access, he would have to compromise two authentication factors—one of which would either be something the user has or something the user is. Significantly increasing the work factor is a powerful deterrent! Additionally, users should be required to reauthenticate periodically during long remote access sessions or after a period of inactivity.

In addition to authenticating the user, remote access devices such as workstations and tablets should be evaluated to ensure they meet the baseline standards required for internal systems. ***Network access control (NAC)*** systems can be used to "check" a remote access device based on defined criteria such as operating system version, security patches, antivirus software version, and wireless and firewall configurations before it is allowed to connect to the infrastructure. If the device does not meet the predefined criteria, the device is denied access.

In Practice

Remote Access Security

Synopsis: To assign responsibility and set the requirements for remote access connections to the internal network.

Policy Statement:

- The Office of Information Security is responsible for approving remote access connections and security controls.
- The Office of Information Technology is responsible for managing and monitoring remote access connection.
- Remote access connections must use 128-bit or greater encryption to protect data in transit (such as VPN, SSL, or SSH).
- Multifactor authentication must be used for remote access. Whenever technically feasible, one factor must be "out of band."
- Remote equipment must be company owned and configured in accordance with company workstation security standards.
- Business partners and vendors wishing to obtain approval for remote access to computing resources must have access approved by the COO. Their company sponsor is required to provide a valid business reason for the remote access to be authorized.
- Employees, business partners, and vendors approved for remote access must be presented with and sign a Remote Access Agreement that acknowledges their responsibilities prior to being granted access.
- Remote access devices must be configured to log successful and failed activity as well as configuration changes.
- Remote access logs must be reviewed daily by the Office of Information Technology or designee, and an activity report must be submitted to the Office of Information Security.
- Remote access user lists must be reviewed quarterly by the Office of Human Resources.

- The result of the review must be reported to both the Office of Information Security and the Office of Information Technology.
- External penetration testing must, at a minimum, be performed semi-annually:
  - The testing is to be conducted by an external independent entity.
  - Selection of the vendor is the responsibility of the Audit Committee.
  - Testing results are to be submitted to the COO.

Teleworking Access Controls

The Telework Enhancement Act of 2010, Public Law 111-292, defines ***teleworking*** as "a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work." In plain language, teleworking allows employees to work offsite, often from their home. According to 2013 research published by MySammy LLC, 20% of the global workforce telecommutes on occasion. Of all teleworkers worldwide, 84% telecommute at least once a month. In the United States, 77% of companies with more than 2,500 employees allow remote working. The Telework Coalition (TelCoa) list of teleworking benefits includes "increased employee productivity and motivation, reduced vehicular pollution, traffic reduction, improved work-life balance, a reduced dependency on imported oil, providing new employment opportunities for the disabled, rural, and older worker, as well as spouses of those in the military and a means to efficiently and effectively establish a decentralized and distributed work force that is necessary as a critical component in business continuity and disaster recovery planning."

Remote locations must be thought of as logical and physical extensions of the internal network and secured appropriately. Controls to ensure the confidentiality, integrity, and availability (CIA) of the information assets and information systems, including monitoring, must be commensurate with the on-premise environment.

NIST SP 880-114: User's Guide to Securing External Devices for Telework and Remote Access provides practical, real-world recommendations for securing telework computers' operating systems (OS) and applications, as well as the home networks that the computers use. It presents basic recommendations for securing consumer devices used for telework. The document also presents advice on protecting the information stored on telework computers and removable media. In addition, it provides tips on considering the security of a device owned by a third party before deciding whether it should be used for telework.

FYI: Yahoo!'s Telecommuting Ban

In February of 2013, Marissa Mayer, the CEO of Yahoo! announced that as of June 2013, Yahoo was ending its support for telecommuting. Here is an excerpt from an internal memo explaining the decision:

"To become the absolute best place to work, communication and collaboration will be important, so we need to be working side-by-side. That is why it is critical that we are all present in our offices. Some of the best decisions and insights come from hallway and cafeteria discussions, meeting new people, and impromptu team meetings. Speed and quality are often sacrificed when we work from home. We need to be one Yahoo!, and that starts with physically being together.

"Beginning in June, we're asking all employees with work-from-home arrangements to work in Yahoo! offices. If this impacts you, your management has already been in touch with next steps. And, for the rest of us who occasionally have to stay home for the cable guy, please use your best judgment in the spirit of collaboration. Being a Yahoo isn't just about your day-to-day job, it is about the interactions and experiences that are only possible in our offices.

"Thanks to all of you, we've already made remarkable progress as a company—and the best is yet to come."

In Practice

Teleworking Policy

Synopsis: To assign responsibility and set the requirements for teleworking.

Policy Statement:

- Teleworking schedule must be requested in writing by management and authorized by the Office of Human Resources.
- The Office of Human Resources is responsible for notifying the Office of Information Security and Office of Information Technology when a user is granted or denied teleworking privileges.
- Teleworking equipment, including connectivity devices, must be company owned and configured in accordance with company security standards.
- The Office of Information Technology is responsible for managing, maintaining, and monitoring the configuration of and the connection to the teleworking location.
- Remote access will be granted in accordance with the remote access policy and standards.
- The teleworker is responsible for the physical security of the telecommuting location.
- Local storage of information classified as "protected" or "confidential" must be authorized by the Office of Information Security.
- Monitoring the teleworker is the responsibility of his or her immediate supervisor.

User Access Controls

The objective of ***user access controls*** is to ensure that authorized users are able to access information and resources while unauthorized users are prevented from access to the same. User access control and management is an enterprise-wide security task. Critical to successful user access management is the involvement of and communication between the Office of Human Resources, the Office of Information Technology, and the Office of Information Security and information system owners.

Why Manage User Access?

User access must be managed in order to maintain confidentiality and data integrity. In keeping with the *least privilege* and *need-to-know* security precepts, users should be provided access to the information and systems needed to do their job and no more. Humans are naturally curious beings. Given unfettered access, we will peek at that which we know we should not. Moreover, user accounts are the first target of a hacker who has gained access to an organization's network. Diligent care must be used when designing procedures for creating accounts and granting access to information.

As discussed in Chapter 6, "Human Resources Security," user provisioning is the process of creating user accounts and group membership, providing company identification and authentication mechanisms, and assigning access rights and permissions. Regardless of the department tasked with the user provisioning process, the information owner is ultimately responsible for authorization and oversight of access. The information owner or designee should review application, folder, or file access controls on a periodic basis. Factors that influence how often reviews should be conducted include the classification of the information being accessed, regulatory requirements, and rate of turnover and/or reorganization of duties. The review should be documented. Issues or inaccuracies should be responded to expediently.

In Practice

User Access Control and Authorization Policy

Synopsis: To define user access control and authorization parameters and responsibilities.

Policy Statement:

- Default user access permissions will be set to "deny all" prior to the appropriation of specific permissions based on role and/or job function.
- Access to company information and systems will only be authorized for workforce personnel with a need-to-know to perform their job function(s).
- Access will be restricted to the minimal amount required to carry out the business requirement of the access.
- An authorization process must be maintained. Permissions must not be granted until the authorization process is complete.

- Information owners are responsible for annually reviewing and reauthorizing user access permissions to data classified as "protected" or "confidential":
  - The Office of Information Security is responsible for managing the review and reauthorization process.
  - An annual report of completion will be provided to the Audit Committee.

Administrative Account Controls

Networks and information systems must be implemented, configured, managed, and monitored. Doing so requires accounts with elevated privileges. Common privileged accounts include network administrators, system administrators, database administrators, firewall administrators, and webmasters. This concentration of power can be dangerous. Mitigating controls include segregation of duties and dual controls. ***Segregation of duties*** requires that tasks be assigned to individuals in a manner such that no one individual can control a process from start to finish. ***Dual control*** requires that two individuals must both complete their half of a specific task. An example of segregation of duties is allowing a security engineer to modify a firewall configuration file but not upload the configuration into the production environment. An example of dual control is requiring two separate keys to unlock a door. Each key is assigned to an individual user. The theory of both controls it that in order to act maliciously, two or more individuals would need to work together. All administrative or privileged account activity should be logged and reviewed.

Administrative accounts should be used only when the activity being performed requires elevated rights and permissions. There is no need to use this type of account to perform routine activities such as checking email, writing reports, performing research on the Internet, and other activities for which a basic user account will suffice. This is important because viruses, worms, and other malicious code will run in the security context of the logged-in user. If a user is logged in as a system administrator and her computer is infected with malicious code, then the criminal that controls the malware has administrative privilege as well. To address this very real risk, every person with a special privilege account should also have a basic user account with which to perform duties that do not require administrative access.

In Practice

Administrative and Privileged Account Policy

Synopsis: To ensure the proper assignment, use, management, and oversight of accounts with administrative or elevated privileges.

Policy Statement:

- Request for assignment of administrator-level accounts or changes to privileged group membership must be submitted to the Office of Information Security and approved by the COO.

- The Office of Information Security is responsible for determining the appropriate use of administrator segregation of duties and dual controls.
- Administrative and privileged user accounts will only be used when performing duties requiring administrative or privileged access.
- All administrative and privileged account holders will have a second user account for performing any function where administrative or privileged access is not required.
- User accounts assigned to contractors, consultants, or service providers who require administrative or privileged access will be enabled according to documented schedule and/or formal request, and disabled at all other times.
- Administrative and privileged account activity will be logged daily and reviewed by the Office of Information Security.
- Administrative and privileged account assignments will be reviewed quarterly by the Office of Information Security.

What Types of Access Should Be Monitored?

Monitoring access and use is a critical component of information security. What is most unfortunate is that many organizations deploy elaborate systems to gather data from many sources and then never look at the data. Mining log data results in a wealth of information that can be used to protect your organization. Log data offers clues about activities that have unexpected and possibly harmful consequences, including the following:

- At-risk events, such as unauthorized access, malware, data leakage, and suspicious activity
- Oversight events, such as reporting on administrative activity, user management, policy changes, remote desktop sessions, configuration changes, and unexpected access
- Security-related operational events, such as reporting on patch installation, software installation, service management, reboots bandwidth utilization, and DNS/DHCP traffic

At a minimum, three categories of user access should be logged and analyzed: successful access, failed access, and privileged operations. ***Successful access*** is a record of user activity. Reporting should include date, time, and action (for example, authenticate, read, delete, or modify). ***Failed access*** is indicative of either unauthorized attempts or authorized user issues. In the first instance, it is important to know whether an intruder is “testing” the system or has launched an attack. In the second, from an operational standpoint, it is important to know if users are having problems logging in, accessing information, or doing their jobs. Oversight of administrative or privileged accounts is critical. Administrators hold the keys to the kingdom. In many organizations, they have unfettered access. Compromise or misuse of administrator accounts can have disastrous consequences.

Is Monitoring Legal?

As we discussed in Chapter 6, employees should have *no expectation of privacy* in respect to actions taken on company time or with company resource. The United States judiciary system has favored employers' right to monitor in order to protect their interests. Among the reasons given in the *Defense Counsel Journal* are the following:

- The work is done at the employer's place of business.
- The employer owns the equipment.
- The employer has an interest in monitoring employee activity to ensure the quality of work.
- The employer has the right to protect property from theft and fraud.

Court rulings suggest that reasonableness is a standard applying to surveillance and monitoring activities. Electronic monitoring is reasonable when there is a business purpose, policies exist to set the privacy expectations of employees, and employees are informed of organizational rules regarding network activities and understand the means used to monitor the workplace.

Acceptable use agreements should include a clause informing users that the company will and does monitor system activity. A commonly accepted practice is to present this statement to system users as a legal warning during the authentication process. Users must agree to company monitoring as a condition of logging on.

In Practice

Monitoring System Access and Use Policy

Synopsis: Monitoring of network activity is necessary to detect unauthorized, suspicious, or at-risk activity.

Policy Statement:

- The Office of Information Technology, the Office of Information Security, and the Office of Human Resources are jointly responsible for determining the extent of logging and analysis required for information systems storing, processing, transmitting, or providing access to information classified as "confidential" or "protected." However, at a minimum the following must be logged:
  - Successful and failed network authentication
  - Successful and failed authentication to any application that stores or processes information classified as "protected"
  - Network and application administrative or privileged account activity
- Exceptions to this list must be authorized by the COO.
- Access logs must be reviewed daily by the Office of Information Technology or designee, and an activity report must be submitted to the Office of Information Security.

FYI: Small Business Note

One of the most significant information security challenges that small businesses face is not having dedicated IT or information security personnel. Very often, someone in the organization with “IT skills” is tapped to install and support critical devices such as firewalls, wireless access points, and networking components. The result is that these devices are often left in their default mode and not properly configured. Of particular concern is when the administrative account password is not changed. Attackers can easily obtain default passwords and take over the device. Passwords can be found in product documentation, and compiled lists are available on the Internet from sites such as www.defaultpassword.com/ and www.routerpasswords.com/.

Summary

Access controls are security features that govern how users and processes communicate and interact with systems and resources. The objective of implementing access controls is to ensure that authorized users and processes are able to access information and resources while unauthorized users and processes are prevented from access to the same. Access control models refer to the active entity that requests access to an object or data as the *subject* and the passive entity being accessed or being acted upon as the *object*.

An organization's approach to access controls is referred to as its *security posture*. There are two fundamental approaches—open and secure. Open, also referred to as *default allow*, means that access not explicitly forbidden is permitted. Secure, also referred to as *default deny*, means that access not explicitly permitted is forbidden. Access decisions should consider the security principles of need-to-know and least privilege. *Need-to-know* means having a demonstrated and authorized reason for being granted access to information. *Least privilege* means granting subjects the minimum level of access required to perform their job or function.

Gaining access is a three-step process. The first step is for the object to recognize the subject. *Identification* is the process of the subject supplying an identifier such as a user name to the object. The next step is to prove that the subject is who they say they are. *Authentication* is the process of the subject supplying verifiable credentials to the object. The last step is determining the actions a subject can take. *Authorization* is the process of assigning authenticated subjects the rights and permissions needed to carry out a specific operation.

Authentication credentials are called *factors*. There are three categories of factors: knowledge (something the user knows), possession (something a user has), and inherence (something the user is). *Single-factor authentication* is when only one factor is presented. *Multifactor authentication* is when two or more factors are presented. *Multilayer authentication* is when two or more of the same type of factors are presented. *Out-of-band authentication* requires communication over a channel that is distinct from the first factor. Data classification, regulatory requirement, the impact of unauthorized access, and the likelihood of a threat being exercised must all be considered when deciding on the level of authentication required.

Once authentication is complete, an authorization model defines how subjects access objects. *Mandatory access controls (MACs)* are defined by policy and cannot be modified by the information owner. *Discretionary access controls (DACs)* are defined by the owner of the object. *Role-based access controls (RBACs)* (also called nondiscretionary) are access permissions based on a specific role or function. In a *rule-based access controls* environment, access is based on criteria that are independent of the user or group account, such as time of day or location.

A *network infrastructure* is defined as an interconnected group of hosts and devices. The infrastructure can be confined to one location or, as often is the case, widely distributed, including branch locations and home offices. *Network segmentation* is the process of logically grouping network assets, resources, and applications in order to stratify authentication requirements and security controls. Segments include enclaves, trusted networks, guest networks, perimeter networks (also referred to as a DMZ), and untrusted networks (including the Internet).

Layered security is the term applied to having different types of security measures designed to work in tandem with a single focus. The focus of layered border security is protecting the internal network from external threats. Firewalls are devices or software that control the flow of traffic between networks using ingress and egress filters. Egress filters can be supplemented by self-generated, open source, or subscription-based IP whitelists or blacklists. *Whitelists* are addresses (IP and/or Internet domain names) of known "good" sites. Conversely, *blacklists* are addresses (IP and/or Internet domain names) of known "bad" sites. Content-filtering applications can be used to restrict access by content category (such as violence, gaming, shopping, or pornography), time factors, application type, bandwidth use, and media. *Intrusion detection systems (IDSs)* are passive devices designed to analyze network traffic in order to detect unauthorized access or malevolent activity. *Intrusion prevention systems (IPSs)* are active devices that sit inline with traffic flow and can respond to identified threats by disabling the connection, dropping the packet, or deleting the malicious content.

The need to access internal corporate network resources from remote location has become increasingly common. Users who work remotely (often from home) on a scheduled basis are referred to as *teleworkers*. VPNs and remote access portals can be used to provide secure remote access for authorized users. A *virtual private network (VPN)* provides a secure tunnel for transmitting data through an unsecured network such as the Internet. *IPsec* (short for IP Security) is a set of protocols developed by the Internet Engineering Task Force (IETF) to support secure exchange of packets at the IP layer and is used by VPN devices.

A remote access portal offers access to one or more applications through a single centralized interface. Both mechanisms authenticate and authorize subjects. Best practices dictate that multifactor authentication is used for remote access connections. *Network access control (NAC)* systems can be used to "check" a remote access device based on defined criteria such as operating system version, security patches, antivirus software and DAT files, and wireless and firewall configurations before it is allowed to connect to the infrastructure.

Organizations are dynamic. New employees are hired, others change roles, some leave under friendly conditions, and others are involuntarily terminated. The objective of user access controls is to ensure that authorized users are able to access information and resources while unauthorized users are prevented from access to the same. Information owners are responsible for the authorization of access and ongoing oversight. Access control reviews should be conducted periodically, commensurate with the classification of the information being accessed, regulatory requirements, and the rate of turnover and/or reorganization of duties.

Access controls are configured and managed by users with administrative or elevated privileges. Although this is necessary, the concentration of power can be dangerous. Mitigating controls include segregation of duties and dual controls. *Segregation of duties* requires that tasks be assigned to individuals in a manner such that no one individual can control a process from start to finish. *Dual control* requires that two individuals must both complete their half of a specific task.

Oversight of user and administrator access reflects best practices and, in many cases, a regulatory requirement. At a minimum, three categories of user access should be logged and analyzed: successful access, failed access, and privileged operations. It is incumbent on the organization to institute a log review process as well as incident responsive procedures for at-risk or suspicious activity.

Access control management policies include Authentication Policy, Access Control Authorization Policy, Network Segmentation Policy, Border Device Security Policy, Remote Access Security Policy, Teleworking Policy, User Access Control and Authorization Policy, Administrative and Privileged Account Policy, and Monitoring System Access and Use Policy.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following terms best describes access controls that are security features that govern how users and processes interact?

   A. Objects
   B. Resources
   C. Processes
   D. All of the above

2. Which of the following terms best describes the process of verifying the identity of a subject?

   A. Accountability
   B. Authorization
   C. Access model
   D. Authentication

3. Which of the following terms best describes the process of assigning authenticated subjects permission to carry out a specific operation?

   A. Accountability
   B. Authorization
   C. Access model
   D. Authentication

4. Which of the following terms best describes the active entity that requests access to an object or data?

   A. Subject
   B. Object
   C. Resource
   D. Factor

5. Which of the following security principles is best described as giving users the minimum access required to do their jobs?

   A. Least access
   B. Less protocol
   C. Least privilege
   D. Least process

6. Which of the following security principles is best described as prohibiting access to information not required for one's work?

   A. Access need security principle
   B. Need-to-monitor security principle
   C. Need-to-know security principle
   D. Required information process security principle

7. Which type of access is allowed by the security principle of default deny?

   A. Basic access is allowed.
   B. Access that is not explicitly forbidden is permitted.
   C. Access that is not explicitly permitted is forbidden.
   D. None of the above.

8. Which of the following statements best describes the access rights of a user who has been granted Top Secret clearance at an organization that is using the mandatory access control (MAC) model?

   A. The user can automatically access all Top Secret information.
   B. The user can access only Top Secret information.
   C. The user can access specific categories of Top Secret information.
   D. The user can only access information up to the Top Secret level.

9. Who is responsible for DAC decisions?

   A. Data owners

   B. Data administrators

   C. Data custodians

   D. Data users

10. Which of the following terms best describes the control that is used when the SOP for user provisioning requires the actions of two systems administrators—one who can create and delete accounts and the other who assigns access permissions?

    A. Least privilege

    B. Segregation of duties

    C. Need to know

    D. Default deny all

11. Which of the following types of network, operating system, or application access controls is user agnostic and relies on specific criteria such as source IP address, time of day, and geographic location?

    A. Mandatory

    B. Role-based

    C. Rule-based

    D. Discretionary

12. Which of the following is not considered an authentication factor?

    A. Knowledge

    B. Inheritance

    C. Possession

    D. Biometric

13. Which of the following terms best describes authentication that requires two or more factors?

    A. Dual control

    B. Multifactor

    C. Multiple-factor

    D. Multilayer

14. Which of the following statements best describes reasons to change a password?

A. Passwords should be changed in order to increase the complexity of the password.

B. Passwords should be changed when there is a suspicion that the password has been compromised.

C. Passwords should be changed in order to create a unique password after a user initially logs on to a system using a default or basic password.

D. All of the above.

15. Which of the following terms best describes a type of password that is a form of knowledge-based authentication that requires a user to answer a question based on something familiar to them?

A. Categorical

B. Cognitive

C. Complex

D. Credential

16. Which of the following types of authentication requires two distinct and separate channels to authenticate?

A. In-band authentication

B. Mobile authentication

C. Out-of-band authentication

D. Out-of-wallet authentication

17. Which of the following terms best describes the internal network that is accessible to authorized users?

A. Trusted network

B. DMZ

C. The Internet

D. Semi-trusted network

18. Rules related to source and destination IP address, port, and protocol are used by a(n) _____ to determine access.

A. firewall

B. IPS

C. IDS

D. VPN

19. Which of the following statements is true of an intrusion detection system (IDS)?

    A. An IDS can disable a connection.
    B. An IDS can respond to identified threats.
    C. An IDS uses signature-based detection and/or anomaly-based detection techniques.
    D. An IDS can delete malicious content.

20. Which of the following terms best describes a VPN?

    A. A VPN provides a secure tunnel for transmitting data through a untrusted network.
    B. A VPN is a cost-effective solution for securing remote access.
    C. Both A and B.
    D. Neither A nor B.

21. Which of the following statements best describes mutual authentication?

    A. Mutual authentication is used to auto-save passwords.
    B. Mutual authentication is used to verify the legitimacy of the server before providing access credentials.
    C. Mutual authentication is used to eliminate the need for multifactor authentication.
    D. Mutual authentication is used to authorize access.

22. Network access controls (NAC) systems are used to "check" a remote device for which of the following?

    A. Operating system version
    B. Patch status
    C. Wireless configuration
    D. All of the above

23. Which of the following statements best describes teleworking?

    A. An employee who talks on the telephone
    B. An employee who uses his cell phone to access the Internet
    C. An employee who works from a remote location on a scheduled basis
    D. An employee who uses a mobile device to check email

24. Which of the following statements is not true of monitoring access?

    A. Monitoring access mitigates the risks associated with misuse of privileges.
    B. Monitoring access is illegal.
    C. Monitoring access can identify user issues.
    D. Monitoring access can provide oversight of administrative activities.

25. The objective of user access controls is to ensure that authorized users are able to access information and resources and that ________________________.

    A. authorized users are able to work uninterrupted

    B. unauthorized users are prevented from accessing information resources

    C. authorized users can access the Internet

    D. unauthorized activity is logged

26. Which of the following statements best describes whitelists?

    A. Whitelists are IP addresses or Internet domain names of sites that are allowed.

    B. Whitelists are IP addresses or Internet domain names of frequently used sites.

    C. Whitelists are IP addresses or Internet domain names of known malware sites.

    D. Whitelists are IP addresses or Internet domain names of sites that should be blocked.

27. Which of the following passwords is the strongest?

    A. PetNameBob

    B. PetN@meB0b

    C. 8579377

    D. H8djwk!!j4

28. Which type of information about user access should be logged and analyzed?

    A. Successful access

    B. Failed access

    C. Privileged operations

    D. All of the above

29. Which of the following types of authentication requires a user to enter a password and answer a question?

    A. Single-factor authentication

    B. Multifactor authentication

    C. Multi-layer authentication

    D. Out-of-band authentication

30. Access logs should be reviewed _______________.

    A. daily

    B. annually

    C. when there is a suspicion of malicious activity

    D. only by law enforcement personnel

EXERCISES

EXERCISE 9.1: Understanding Access Control Concepts

1. Define the following access control management terminology:

	Term	Definition
1.1	Access control	
1.2	Authentication	
1.3	Authorization	
1.4	Default deny	
1.5	Default allow	
1.6	Least privilege	
1.7	Need-to-know	
1.8	Mandatory access control (MAC)	
1.9	Discretionary access control (DAC)	
1.10	Network access control (NAC)	

2. Provide an example of an authentication control that affects you.
3. Provide an example of an authorization control that affects you.

EXERCISE 9.2: Managing User Accounts and Passwords

1. How many authentication factors does the email program you use require?
2. What are the required password characteristics for the email program you use? Include length, complexity, expiration, and banned words or phrases.
3. In your opinion, are the requirements adequate?

EXERCISE 9.3: Understanding Multifactor and Mutual Authentication

1. Find an image of or take a picture of a possession or inherence authentication device.
2. Find and describe an example of mutual authentication.
3. Explain how one of the preceding works.

EXERCISE 9.4: Analyzing Firewall Rule Sets

Firewall rule sets use source IP addresses, destination addresses, ports, and protocols.

1. Describe the function of each.
2. What is the purpose of the following rule?

   Allow Src=10.1.23.54 dest=85.75.32.200 Proto=tcp 21

3. What is the purpose of the following rule?

   Deny Src=ANY dest=ANY Proto=tcp 23

EXERCISE 9.5: Granting Administrative Access

1. Do you have administrative rights on your laptop, workstation, or tablet?
2. If yes, do you have the option to also have a normal user account? If no, who does?
3. Explain what is meant by the phrase "security context of the currently logged-in user."

PROJECTS

PROJECT 9.1: Creating an RFP for Penetration Testing

You have been asked to send out a Red Team penetration testing Request for Proposal (RFP) document.

1. Explain what is meant by "Red Team."
2. Find three companies to send the RFP to. Explain why you chose them.
3. The selected vendor will potentially have access to your network. What due diligence criteria should be included in the vendor-selection process? Select one of the companies from the previous step and find out as much as you can about them (for example, reputation, history, credentials).

PROJECT 9.2: Reviewing User Access Permissions

Reviewing user access permissions can be a time-consuming and resource-intensive process and is generally reserved for applications or systems that have information classified as "protected" or "confidential."

1. Should the student portal at your school be subject to an annual user access permission audit? If yes, why? If no, why not?
2. Automating review processes contribute to efficiency and accuracy. Research options for automating the user access review process and make a recommendation.

PROJECT 9.3: Developing Telecommuting Best Practices

Your organization has decided to allow users the option of working from home.

1. Make a list of six security issues that must be considered.
2. Note your recommendations for each issue and detail any associated security control.
3. Assume that your recommendations have been accepted. You have now been tasked with training teleworkers. Create a presentation that explains "work from home" security best practices.

Case Study

Assessing the RSA Cyber Attack

In March of 2011, EMC Corp's RSA unit disclosed that it had been the victim of a successful cyber attack. The criminals targeted proprietary RSA SecureID Token information that could be used to breach the network security of defense contractors and government organizations.

Research this incident and answer the following questions:

1. How did the criminals get access to the RSA network?
2. Why was the attack successful? What controls were missing that may have prevented or detected the attack?
3. How was defense contractor Lockheed Martin impacted?
4. How much did the breach cost RSA? What are the estimated costs to RSA customers?

References

Regulations Cited

"Supplement to Authentication in an Internet Banking Environment," issued by the Federal Institutions Examination Council, 6/28/2011.

"The Telework Enhancement Act of 2010, Public Law 111-292," official website of the Government Printing Office, accessed 07/2013, www.gpo.gov/fdsys/pkg/PLAW-111publ292/.../PLAW-111publ292.pdf.

Other References

"IDS vs. IPS Explained," accessed 07/2013, /www.comparebusinessproducts.com/fyi/ids-vs-ips.

"Mandatory, Discretionary, Role and Rule Based Access Control," accessed 07/2013, www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control.

Mohindra, Dhruv. "POS02-C. Follow the principle of least privilege," accessed 07/2013, www.securecoding.cert.org/confluence/display/seccode/POS02-C.+Follow+the+principle+of+least+privilege.

Nilssonandeers. "Statistics of 450,000 leaked Yahoo Accounts," Pastebin, accessed 07/2013, http://pastebin.com/2D6bHGTa.

Protalinski, Emil, "Yahoo Hack: Is yours one of them?" *ZDNet*, July 12, 2012, accessed 07/2013, www.zdnet.com/the-top-10-passwords-from-the-yahoo-hack-is-yours-one-of-them-7000000815/.

Saltzer, J. H. and Schroeder, M. D. "The Protection of Information in Computer Systems," Proceedings of the IEEE, Vol. 63, No. 9 (Sept. 1975).

“The Telecommuter Infographic, An Analysis of the World’s Remote Workforce,” MySammy LLC, accessed 07/2013, www.mysammy.com/infographics-telecommuter.

“Our Vision and Mission,” TelCoa, accessed 07/2013, www.telcoa.org/about-us/our-vision-and-mission/.

“What is Telecommuting?” Emory University WorkLife Resource Center, accessed 07/2013, www.worklife.emory.edu/workplaceflexibility/telecommuting/whatis.html.

This page intentionally left blank

Chapter 10

Information Systems Acquisition, Development, and Maintenance

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Understand the rationale for the systems development lifecycle (SDLC).
- Recognize the stages of software releases.
- Appreciate the importance of developing secure code.
- Be aware of the most common application development security faults.
- Explain cryptographic components.
- Develop policies related to systems acquisition, development, and maintenance.

Section 14 of ISO 27002:2013: Information Systems Acquisition, Development, and Maintenance (ISADM) focuses on the security requirements of information systems, application, and code from conception to destruction. This sequence is referred to as the systems development lifecycle (SDLC). Particular emphasis is put on vulnerability management to ensure integrity, cryptographic controls to ensure integrity and confidentiality, and security of system files to ensure confidentiality, integrity, and availability (CIA). The domain constructs apply to in-house, outsourced, and commercially developed systems, applications, and code. Section 10 of ISO 27002:2013: Cryptography focuses on proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. Because cryptographic protection mechanisms are closely related to information systems development and maintenance, it is included in this chapter.

Of all the security domains we have discussed so far, this one has the most widespread implications. Most cybercrime is opportunistic, meaning that the criminals take advantage of the system vulnerabilities. Information systems, applications, and code that does not have embedded security controls all expose the organization to undue risk. Consider a company that relies on a web-based application linked to a back-end database. If the code used to create the web-based application was not thoroughly vetted, it may contain vulnerabilities that would allow a hacker to bring down the application with a denial of service (DoS) attack, run code on the server hosting the application, or even trick the database into publishing classified information. These events harm an organization's reputation, create compliance and legal issues, and significantly impact the bottom line.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 10 of ISO 27002:2013, the cryptography domain, focuses on proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. Section 14 of ISO 27002:2013, the ISADM domain, focuses on the security requirements of information systems, applications, and code, from conception to destruction.

Corresponding NIST guidance is provided in the following documents:

- SP 800-23: Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- SP 800-57: Recommendations for Key Management—Part 1: General (Revision 3)
- SP 800-57: Recommendations for Key Management—Part 2: Best Practices for Key Management Organization
- SP 800-57: Recommendations for Key Management—Part 3: Application-Specific Key Management Guidance
- SP 800-64: Security Considerations in the System Development Life Cycle
- SP 800-111: Guide to Storage Encryption Technologies for End User Devices

System Security Requirements

Security should be a priority objective during the design and acquisition phases of any new information system, application, or code development. Attempting to retrofit security is expensive, resource intensive, and all too often does not work. "Productivity requirements" and/or the "rush to market" often preclude a thorough security analysis, which is unfortunate because it has been proven time and time again that early-stage identification of security requirements is both cost effective and efficient. Utilizing a structured development process increases the probability that security objectives will be achieved.

What Is SDLC?

The ***systems development lifecycle (SDLC)*** provides a standardized process for all phases of any system development or acquisition effort. As defined by NIST, an SDLC includes five phases: initiation, development/acquisition, implementation, operational, and disposal.

- During the ***initiation*** phase, the need for a system is expressed and the purpose of the system is documented.
- During the ***development/acquisition*** phase, the system is designed, purchased, programmed, developed, or otherwise constructed.
- The ***implementation*** phase includes system testing, modification if necessary, retesting if modified, and finally acceptance.
- During the ***operational*** phase, the system is put into production. The system is almost always modified by the addition of hardware and software and by numerous other events. Monitoring, auditing, and testing should be ongoing.
- Activities conducted during the ***disposal*** phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system.

Each phase includes a minimum set of tasks needed to effectively incorporate security in the system development process. Phases may continue to be repeated throughout a system's life prior to disposal.

Initiation Phase

During the initiation phase, the organization establishes the need for a system and documents its purpose. Security planning must begin in the initiation phase. The information to be processed, transmitted, or stored is evaluated for CIA security requirements, as well as the security and criticality requirements of the information system. It is essential that all stakeholders have a common understanding of the security considerations. This early involvement will enable the developers or purchasing managers to plan security requirements and associated constraints into the project. It also reminds project leaders that many decisions being made have security implications that should be weighed appropriately, as the project continues. Other tasks that should be addressed in the initiation phase include assignment of roles and responsibilities, identification of compliance requirements, decisions on security metrics and testing, and the systems acceptance process.

Development/Acquisition Phase

During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. A key security activity in this phase is conducting a risk assessment. In addition, the organization should analyze security requirements, perform functional and security testing, and design the security architecture. Both the ISO standard and NIST emphasize the importance of conducting risk assessments to evaluate the security requirements for new systems and upgrades. The aim is to identify potential risks associated with the project and to use this information to select baseline security controls. The risk assessment process is iterative and needs to be repeated whenever a new functional requirement is introduced. As they are determined, security control requirements become part of the project security plan. Security controls must be tested to ensure they perform as intended.

Implementation Phase

In the implementation phase, the organization configures and enables system security features, tests the functionality of these features, installs or implements the system, and obtains a formal authorization to operate the system. Design reviews and system tests should be performed before placing the system into operation to ensure that it meets all required security specifications. It is important that adequate time be built into the project plan to address any findings, modify the system or software, and retest.

The final task in this phase is authorization. It is the responsibility of the system owner or designee to green light the implementation and allow the system to be placed in production mode. In the federal government, this process is known as ***certification and accreditation (C&A)***. OMB Circular A-130 requires the security authorization of an information system to process, store, or transmit information. The authorizing official relies primarily on the completed system security plan, the inherent risk as determined by the risk assessment, and the security test results.

Operational/Maintenance Phase

In this phase, systems and products are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and software components are added or replaced. Configuration management and change control processes are essential to ensure that required security controls are maintained. The organization should continuously monitor performance of the system to ensure that it is consistent with pre-established user and security requirements, and that needed system modifications are incorporated. Periodic testing and evaluation of the security controls in an information system must be conducted to ensure continued effectiveness and to identify any new vulnerabilities that may have been introduced or recently discovered. Vulnerabilities identified after implementation cannot simply be ignored. Depending on the severity of the finding, it may be possible to implement compensating controls while "fixes" are being developed. There may be situations that require the system to be taken offline until the vulnerabilities can be mitigated.

Disposal Phase

Often, there is no definitive end or retirement of an information system or code. Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information for the original system should still be relevant and useful when the organization develops the security plan for the follow-on system. When the time does come to discard system information, hardware, and software, it must not result in the unauthorized disclosure of protected or confidential data. Disposal activities archiving information, sanitization of media, and disposal of hardware components must be done in accordance with the organization's destruction and disposal requirements and policies.

In Practice

Systems Development Lifecycle (SDLC) Policy

Synopsis: Ensure a structured and standardized process for all phases of system development/acquisition efforts, which includes security considerations, requirements, and testing.

Policy Statement:

- The Office of Information Technology is responsible for adopting, implementing, and requiring compliance with an SDLC process and workflow. The SDLC must define initiation, development/acquisition, implementation, operations, and disposal requirements.
- At each phase, security requirements must be evaluated and, as appropriate, security controls tested.
- The system owner, in conjunction with the Office of Information Security, is responsible for defining system security requirements.
- The system owner, in conjunction with the Office of Information Security, is responsible for authorizing production systems prior to implementation.
- If necessary, independent experts may be brought in to evaluate the project or any component thereof.

What about Commercially Available or Open Source Software?

SDLC principles apply to commercially available software—sometimes referred to as ***commercial off-the-shelf software (COTS)***—and to open source software. The primary difference is that the development is not done in-house. Commercial software should be evaluated to make sure it meets or exceeds the organization's security requirement. Because software is often released in stages, it is important to be aware of and understand the release stages. Only stable and tested software releases should be deployed on production servers to protect data availability and data integrity. Operating system and application updates should not be deployed until they have been thoroughly tested in a lab environment and declared safe to be released in a production environment. Once installed, all software and applications should be included in internal vulnerability testing.

Software Releases

The ***alpha phase*** is the initial release of software for testing. Alpha software can be unstable and can cause crashes or data loss. External availability of alpha software is uncommon in proprietary software. However, open source software, in particular, often has publicly available alpha versions, often distributed as the raw source code of the software. ***Beta phase*** indicates that the software is feature complete and the focus is usability testing. A ***release candidate (RC)*** is a hybrid of a beta and a final release version. It has the potential to be the final release unless significant issues are identified. ***General availability*** or ***go live*** is when the software has been made commercially available and is in general distribution. Alpha, beta, and RCs have a tendency to be unstable and unpredictable and are not suitable for a production environment. This unpredictability can have devastating consequences, including data exposures, data loss, data corruption, and unplanned downtime.

Software Updates

During its supported lifetime, software is sometimes updated. Updates are different from security patches. ***Security patches*** are designed to address a specific vulnerability and are applied in accordance with the patch management policy. ***Updates*** generally include functional enhancements and new features. Updates should be subject to the organization's change management process and should be thoroughly tested before being implemented in a production environment. This is true for both operating systems and applications. For example, a new system utility might work perfectly with 99% of applications, but what if a critical line-of-business application deployed on the same server falls in the remaining 1%? This can have a disastrous effect on the availability, and potentially on the integrity, of the data. This risk, however minimal it may appear, must not be ignored. Even when an update has been thoroughly tested, organizations still need to prepare for the unforeseen and make sure they have a documented ***rollback strategy*** to return to the previous stable state in case problems occur.

If an update requires a system reboot, it should be delayed until the reboot will have the least impact on business productivity. Typically, this means after hours or on weekends, although if a company is international and has users who rely on data located in different time zones, this can get a bit tricky. If an update does not require a system reboot, but will still severely impact the level of system performance, it should also be delayed until it will have the least impact on business productivity.

The Testing Environment

The worst-case scenario for a testing environment is that a company simply does not have one, and is willing to have production servers double as test servers. Best-case scenario, the testing environment is set up as a mirror image of the production environment, software and hardware included. The closer to the production environment the test environment is, the more the test results can be trusted. A cost/benefit analysis that takes into consideration the probability and associated costs of downtime, data loss, and integrity loss will determine how much should be invested in a test or staging environment.

Protecting Test Data

Consider a medical practice with an electronic medical records (EMR) database replete with patient information. Imagine the security measures that have been put in place to make sure the CIA of the data is protected. Because this database is pretty much the lifeblood of this practice and is protected under law, it is to be expected that those security measures are extensive. Live data should never be used in a test environment because it is highly unlikely that the same level of data protection has been implemented, and exposure of protected data would be a serious violation of patient confidentiality and regulatory requirements. Instead, either de-identified data or dummy data should be used. ***De-identification*** is the process of removing information that would identify the source or subject of the data. Strategies include deleting or masking the name, social security number, date of birth, and demographics. ***Dummy data*** is, in essence, fictional. For example, rather than using actual patient data to test an EMR database, the medical practice would enter fake patient data into the system. That way, the application could be tested with no violation of confidentiality.

In Practice

System Implementation and Update Policy

Synopsis: Define the requirements for the implementation and maintenance of commercial and open source software.

Policy Statement:

- Operating systems and applications (collectively referred to as “system”) implementation and updates must follow the company’s change management process.
- Without exception, alpha, beta, or prerelease applications must not be deployed on production systems.
- It is the joint responsibility of the Office of Information Security and the Office of Information Technology to test system implementation and updates prior to deployment in the production environment.
- The Office of Information Technology is responsible for budgeting for and maintaining a test environment that is representative of the production environment.
- Without exception, data classified as “protected” must not be used in a test environment unless it has been de-identified. It is the responsibility of the Office of Information Security to approve the de-identification schema.

Secure Code

The two types of code are insecure code (sometimes referred to as “sloppy code”) and secure code. ***Insecure code*** is sometimes the result of an amateurish effort, but more often than not, it reflects a flawed process. ***Secure code***, however, is always the result of a deliberate process that prioritized security from the beginning of the design phase onward.

FYI: Open SAMM

The ***Software Assurance Maturity Model (SAMM)*** is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM (www.opensamm.org/) will aid in the following:

- Evaluating an organization's existing software security practices
- Building a balanced software security assurance program in well-defined iterations
- Demonstrating concrete improvements to a security assurance program
- Defining and measuring security-related activities throughout an organization

SAMM was defined with flexibility in mind such that it can be utilized by small, medium, and large organizations using any style of development. Additionally, this model can be applied organization-wide, for a single line of business, or even for an individual project. Beyond these traits, SAMM was built on the following principles:

- *An organization's behavior changes slowly over time*. A successful software security program should be specified in small iterations that deliver tangible assurance gains while incrementally working toward long-term goals.
- *There is no single recipe that works for all organizations*. A software security framework must be flexible and allow organizations to tailor their choices based on their risk tolerance and the way in which they build and use software.
- *Guidance related to security activities must be prescriptive*. All the steps in building and assessing an assurance program should be simple, well defined, and measurable. This model also provides roadmap templates for common types of organizations.

Source: OWASP.org (https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model)

The Open Web Application Security Project (OWASP)

Deploying secure code is the responsibility of the system owner. A number of secure coding resources are available for system owners, project managers, developers, programmers, and information security professionals. One of the most well respected and widely utilized is OWASP. The ***Open Web Application Security Project (OWASP)*** is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. Everyone is free to participate in OWASP, and all of its materials are available under a free and open software license. On a three-year cycle, beginning in 2004, OWASP releases the "OWASP Top Ten." The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. The information is applicable to a spectrum of non-web applications, operating systems, and databases. Project members include a variety of security experts from around the world who have shared their expertise to produce this list. The most recent list was published in 2013. The 2013 and 2010 lists both cite injection flaws as the number-one security issue.

FYI: 2013 OWASP Top Ten Application Web Application Security Flaws

The OWASP Top 10 are considerd the ten most critical web application security risks:

A1 – Injection

A2 – Broken Authentication and Session Management

A3 – Cross-site Scripting (XSS)

A4 – Insecure Direct Object Reference

A5 – Security Misconfiguration

A6 – Sensitive Data Exposure

A7 – Missing Function Level Access Control

A8 – Cross-site Request Forgery (CRSF)

A9 – Using Component with Known Vulnerabilities

A10 – Unvalidated Redirects and Forwards

The complete list, which includes detailed explanation and examples, is published on the OWASP website www.owasp.org).

What Is Injection?

The most common web application security flaw is the failure to properly validate input from the client or environment. OWASP defines ***injection*** as when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing an unintended command or accessing data without proper authorization. The attacker can be anyone who can send data to the systems, including internal users, external users, and administrators. The attack is simply a data string designed to exploit the code vulnerability. Injection flaws are particularly common in older code. A successful attack can result in data loss, corruption, compromise, or DoS. Preventing injection requires keeping untrusted data separate from commands and queries.

Input Validation

Input validation is the process of validating all the input to an application before using it. This includes correct syntax, length, characters, and ranges. Consider a web page with a simple form that contains fields corresponding to your physical address information, such as Street Name, ZIP Code, and so on. Once you click the "submit" button, the information you entered in the fields is sent to the web server and entered into a back-end database. The objective of input validation is to evaluate the format of entered information and, when appropriate, deny the input. To continue our example, let's focus on the ZIP Code field. Zip Codes consist of numbers only, and the basic ones only include five digits. Input validation would look at how many and what type of characters are entered in the field. In this case, the first section of the ZIP Code field would require five numeric characters. This limitation would prevent the user from entering more or less than five characters as well as nonnumeric characters. This strategy is known as *whitelist* or *positive validation*.

You may wonder, why bother to go through all this? Who cares if a user sends the wrong ZIP Code? Who cares if the information entered in the ZIP Code field includes letters and/or ASCII characters? Hackers care. Hackers attempt to pass code in those fields to see how the database will react. They want to see if they can bring down the application (DoS attack against that application), bring down the server on which it resides (DoS against the server, and therefore against all the applications that reside on that server), or run code on the target server to manipulate or publish sensitive data. Proper input validation is therefore a way to limit the ability of a hacker to try and "abuse" an application system.

Dynamic Data Verification

Many application systems are designed to rely on outside parameter tables for dynamic data. ***Dynamic data*** is defined as data that changes as updates become available—for example, an e-commerce application that automatically calculates sales tax based on the ZIP Code entered. The process of checking that the sales tax rate entered is indeed the one that matches the state entered by the customer is another form of input validation. What is tricky in this type of situation is that the information pulled from the outside table is real and legitimate—it is just that it does not apply to the situation at hand. This is a lot harder to track than when the data input is clearly wrong, such as when a letter is entered in a ZIP Code field.

Dynamic data is used by numerous application systems. A simple example of this is the exchange rate for a particular currency. These values continually change, and using the correct value is critical. If the transaction involves a large sum, the difference can translate into a fair amount of money! Data validation extends to verification that the business rule is also correct.

Output Validation

Output validation is the process of validating (and in some cases, masking) the output of a process before it is provided to the recipient. An example would be substituting asterisks for numbers on a credit card receipt. Output validation controls what information is exposed or provided. You need to be aware of output validation, however, especially as it relates to hacker discovery techniques. Hackers look for clues and then use this information as part of the footprinting process. One of the first things a hacker looks to learn about a targeted application is how it reacts to systematic abuse of the interface. A hacker will learn a lot about how the application reacts to errors if the developers did not run output validation tests prior to deployment. They may, for example, learn that a certain application is vulnerable to SQL injection attacks, buffer overflow attacks, and so on. The answer an application gives about an error is potentially a pointer that can lead to vulnerability, and a hacker will try to make that application "talk" to better customize the attack.

Developers test applications by feeding erroneous data into the interface to see how it reacts and what it reveals. This feedback is used to modify the code with the objective of producing a secure application. The more time spent on testing, the less likely hackers will gain the advantage.

Why Is Broken Authentication and Session Management Important?

Number two on the 2013 OWASP list is broken authentication and session management. If session management assets such as user credentials and session IDs are not properly protected, the session can be hijacked or taken over by a malicious intruder. When authentication credentials are stored or transmitted in clear text or when credentials can be guessed or overwritten through weak account management functions (for example, account creation, change password, recover password, weak session IDs), the identity of the authorized user can be impersonated. If session IDs are exposed in the URL, do not time out, or are not invalidated after successful logoff, malicious intruders have the opportunity to continue an authenticated session. A critical security design requirement must be strong authentication and session management controls. A common control for protecting authentication credentials and session IDs is encryption. We discussed authentication in Chapter 9, "Access Control Management." We will examine encryption and the field of cryptography in the next section of this chapter.

In Practice

Application Development Policy

Synopsis: Define code and application development security requirements.

Policy Statement:

- System owners are responsible for oversight of secure code development.
- Security requirements must be defined and documented during the application development initiation phase.
- Code development will be done in accordance with industry best practices.
- Developers will be provided with adequate training, resources, and time.
- At the discretion of the system owner and with the approval of the Office of Information Security, third parties may be engaged to design, develop, and test internal applications.
- All code developed or customized must be tested and validated during development, prior to release, and whenever a change is implemented.
- The Office of Information Security is responsible for certifying the results of testing and accreditation to move to the next phase.

Cryptography

The art and science of writing secret information is called ***cryptography***. The origin of the term involves the Greek words *kryptos* meaning "hidden" and *graphia* meaning "writing." Three distinct goals are associated with cryptography:

- **Confidentiality**—Unauthorized parties cannot access the data. Data can be *encrypted*, which provides confidentiality.

- **Integrity**—Assurance is provided that the data was not modified. Data can be *hashed*, which provides integrity.
- **Authenticity/nonrepudiation**—The source of the data is validated. Data can be *digitally signed*, which ensures authentication/nonrepudiation and integrity.

Data can be encrypted and digitally signed, which provides for confidentiality, authentication, and integrity.

Encryption is the conversion of plain text into what is known as *cipher text* using an algorithm called a *cipher*. ***Cipher text*** is text that is unreadable by a human or computer. ***Decryption***, the inverse of encryption, is the process of turning cipher text back into readable plain text. Encryption and decryption require the use of a secret key. The ***key*** is a value that specifies what part of the algorithm to apply, in what order, and what variables to input. Similar to authentication passwords, it is critical to use a strong key that cannot be discovered and to protect the key from unauthorized access. Protecting the key is generally referred to as ***key management***. We are going to be examining the use of symmetric and asymmetric keys as well as key management later in this chapter.

Ensuring that a message has not been changed in any way during transmission is referred to as ***message integrity***. ***Hashing*** is the process of creating a numeric value that represents the original text. A hash function (such as SHA or MD5) takes a variable size input and produces a fixed size output. The output is referred to as a hash value, message digest, or fingerprint. Unlike encryption, hashing is a one-way process, meaning that the hash value is never turned back into plain text. If the original data has not changed, the hash function should always produce the same value. Comparing the values confirms the integrity of the message. Used alone, hashing provides message integrity and not confidentiality or authentication.

A ***digital signature*** is a hash value (message digest) that has been encrypted with the sender's private key. The hash must be decrypted with the corresponding key. This proves the identity of the sender. The hash values are then compared to prove the message integrity. Digital signatures provide authenticity/nonrepudiation and message integrity. Nonrepudiation means that the sender cannot deny that the message came from them.

FYI: The Caesar Cipher

The need for secure communication is certainly not new. The Roman ruler Julius Caesar (100 B.C.–44 B.C.) used a cipher for secret battlefield communication. He substituted each letter of the alphabet with a letter three positions further along. Later, any cipher that used this "displacement" concept for the creation of a cipher alphabet was referred to as a Caesar cipher. Of all the substitution-type ciphers, this Caesar cipher is the simplest to solve because there are only 25 possible combinations.

Standard alphabet:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Caesar alphabet:

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

For example, using the Caesar cipher system, the message THE ENEMY IS NEAR would be written as **QEB BKBJV FP KBXO**.

Why Encrypt?

Encryption protects the confidentiality of data at rest and in transit. There are a wide variety of encryption algorithms, techniques, and products. Encryption can be applied granularly, such as to an individual file, or broadly, such as encrypting all stored or transmitted data. Per NIST, the appropriate encryption solution for a particular situation depends primarily on the type of storage, the amount of information that needs to be protected, the environments where the storage will be located, and the threats that need to be mitigated. The three classes of storage ("at rest") encryption techniques are full disk encryption, volume and virtual disk encryption, and file/folder encryption. The array of in-transit encryptions protocols and technologies include TLS/SSL (HTTPS), WEP and WPA, VPN, and IPsec. Protecting information in transit safeguards the data as it traverses a wired or wireless network. The current standard specification for encrypting electronic data is the Advanced Encryption Standard (AES). Almost all known attacks against AES's underlying algorithm are computationally infeasible.

Regulatory Requirements

In addition to being a best practice, the need for encryption is cited in numerous federal regulations, including the Gramm-Leach-Bliley Act (GLBA) and HIPAA/HITECH. At the state level, multiple states (including Massachusetts, Nevada, and Washington) have statues requiring encryption. Massachusetts 201 CMR17 requires encryption of all transmitted records and files containing personal information that will travel across public networks, encryption of all data containing personal information to be transmitted wirelessly, as well as encryption of all personal information stored on laptops or other portable devices. Nevada NRS 603A requires encryption of credit and debit card data as well as encryption of mobile devices and media. Washington HB 2574 requires that personal information, including name combined with social security number, driver's license number, and financial account information, be encrypted if it is transmitted or stored on the Internet.

What Is a "Key"?

A ***key*** is a secret code that is used by a cryptographic algorithm. It provides the instructions that result in the functional output. Cryptographic algorithms themselves are generally known. It is the secrecy of the key that provides for security. The number of possible keys that can be used with an algorithm is known as the ***keyspace***, which is a large set of random values that the algorithm chooses from when it needs to make a key. The larger the keyspace, the more possibilities for different keys. For example, if an algorithm uses a key that is a string of 10 bits, then its key space is the set of all binary strings of length 10, which results in a keyspace size of 2^{10} (or 1,024); a 40-bit key results in 2^{40} possible values; and a 256-bit key results in 2^{256} possible values. Longer keys are harder to break, but require more computation and processing power. Two factors must be taken into consideration when deciding upon the key length: the desired level of protection and the amount of resources available.

Symmetric Keys

A ***symmetric key*** algorithm uses a single secret key, which must be shared in advance and kept private by both the sender and the receiver. Symmetric keys are often referred to as a *shared key*. Because the keys are shared, symmetric algorithms cannot be used to provide nonrepudiation or authenticity. The most well-known symmetric algorithm is DES. The strength of symmetric keys is that they are computationally efficient. The weakness is that key management is inherently insecure and that it is not scalable, because a unique key set must be used in order to protect the secrecy of the key.

Asymmetric Keys

Asymmetric key cryptography, also as known as ***public key*** cryptography, uses two different but mathematically related keys known as *public* and *private* keys. Think of public and private keys as two keys to the same lock—one used to lock and the other to unlock. The private key never leaves the owner's possession. The public key is given out freely. The public key is used to encrypt plain text or to verify a digital signature, whereas the private key is used to decrypt cipher text or to create a digital signature. Asymmetric key technologies allow for efficient, scalable, and secure key distribution; however, they are computationally resource intensive.

What Is PKI?

Public Key Infrastructure (PKI) is the framework and services used to create, distribute, manage, and revoke public keys. PKI is made up of multiple components, including a Certification Authority (CA), a Registration Authority (RA), client nodes, and the digital certificate itself:

- The ***Certification Authority (CA)*** issues and maintains digital certificates.
- The ***Registration Authority (RA)*** performs the administrative functions, including verifying the identity of users and organizations requesting a digital certificate, renewing certificates, and revoking certificates.
- ***Client nodes*** are interfaces for users, devices, and applications to access PKI functions, including the requesting of certificates and other keying material. They may include cryptographic modules, software, and procedures necessary to provide user access to the PKI.
- A ***digital certificate*** is used to associate a public key with an identity. Certificates include the certificate holder's public key, serial number of the certificate, certificate holder's distinguished name, certificate validity period, unique name of the certificate issuer, digital signature of the issuer, and signature algorithm identifier.

FYI: Viewing a Digital Certificate

If you are using an Apple Mac operating system, the certificates are stored in the Keychain Access utility. If you are using a Microsoft Windows operating system, digital certificates are stored in the Internet Browser application. To view these certificates in Internet Explorer, go to the Internet Options Content tab and click the Certificates button. To view them in Firefox, go to Options, Advanced, Certificates tab.

Why Protect Cryptographic Keys?

As mentioned earlier in the chapter, the usefulness of a cryptographic system is entirely dependent on the secrecy and management of the key. This is so important that NIST has published a three-part document devoted to cryptographic key management guidance. SP 800-67: Recommendations for Key Management, Part 1: General (Revision 3) provides general guidance and best practices for the management of cryptographic keying material. Part 2: Best Practices for Key Management Organization provides guidance on policy and security planning requirements for U.S. government agencies. Part 3: Application Specific Key Management Guidance provides guidance when using the cryptographic features of current systems. In the Overview of Part 1, NIST describes the importance of key management as follows: "The proper management of cryptographic keys is essential to the effective use of cryptography for security. Keys are analogous to the combination of a safe. If a safe combination is known to an adversary, the strongest safe provides no security against penetration. Similarly, poor key management may easily compromise strong algorithms. Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded to the keys. All keys need to be protected against modification, and secret and private keys need to be protected against unauthorized disclosure. Key management provides the foundation for the secure generation, storage, distribution, use, and destruction of keys."

Best practices for key management include the following:

- The key length should be long enough to provide the necessary level of protection.
- Keys should be transmitted and stored by secure means.
- Key values should be random, and the full spectrum of the keyspace should be used.
- The key's lifetime should correspond with the sensitivity of the data it is protecting.
- Keys should be backed up in case of emergency. However, multiple copies of keys increase the chance of disclosure and compromise.
- Keys should be properly destroyed when their lifetime ends.
- Keys should never be presented in clear text.

Key management policy and standards should include assigned responsibility for key management, the nature of information to be protected, the classes of threats, the cryptographic protection mechanisms to be used, and the protection requirements for the key and associated processes.

Digital Certificate Compromise

Certification Authorities (CAs) have increasingly become targets for sophisticated cyber attacks. An attacker who breaches a CA to generate and obtain fraudulent certificates can then use the fraudulent certificates to impersonate an individual or organization. In July of 2012, NIST issued an ITL bulletin titled "Preparing for and Responding to Certification Compromise and Fraudulent Certificate Issue." The bulletin primarily focuses on guidance for Certification and Registration Authorities. The bulletin does, however, include the guidance for any organization impacted by the fraud.

The built-in defense against a fraudulently issued certificate is certificate revocation. When a rouge or fraudulent certificate is identified, the CA will issue and distribute a certificate revocation list. Alternatively, a browser may be configured to use the Online Certificate Status Protocol (OCSP) to obtain revocation status.

In Practice

Key Management Policy

Synopsis: To assign responsibility for key management and cryptographic standards.

Policy Statement:

- The Office of Information Security is responsible for key management, including but not limited to algorithm decisions, key length, key security and resiliency, requesting and maintaining digital certificates, as well as user education. The Office of Information Security will publish cryptographic standards.
- The Office of Information Technology is responsible for implementation and operational management of cryptographic technologies.
- Without exception, encryption is required whenever protected or confidential information is transmitted externally. This includes email and files transfer. The encryption mechanism must be NIST approved.
- Without exception, all portable media that stores or has the potential to store protected or confidential information must be encrypted. The encryption mechanism must be NIST approved.
- Data at rest must be encrypted regardless of media when required by state and/or federal regulation or contractual agreement.
- At all times, passwords and PINs must be stored and transmitted as cipher text.

FYI: Small Business Note

Encryption keeps valuable data safe. Every organization, irrespective of size, should encrypt the following if there is any chance that legally protected or company confidential data will be stored or transmitted:

- Mobile devices such as laptops, tablets, smartphones
- Removable media such as USB drives and backup tapes
- Internet traffic such as file transfer or email
- Remote access to the company network
- Wireless transmission

When creating the “secure key,” make sure to use a long random string of numbers, letters, and special characters.

Summary

Whether they are developed in house, purchased, or open source, companies rely on line-of-business applications. This reliance implies that the availability of those solutions must be protected to avoid severe losses in revenue, the integrity must be protected to avoid unauthorized modification, and the confidentiality must be protected to honor the public trust and maintain compliance with regulatory requirements.

Custom applications should be built with security in mind from the start. Adopting an SDLC methodology that integrates security considerations ensures that this objective is met. The SDLC provides a structured and standardized process for all phases of any system development effort. During the initiation phase, the need for a system is expressed and the purpose of the system is documented. During the development/acquisition phase, the system is designed, purchased, programmed, developed, or otherwise constructed. During the implementation phase, the system is tested, modified if necessary, retested if modified, and finally accepted. During the operational phase, the system is put into production. Monitoring, auditing, and testing should be ongoing. Activities conducted during the disposal phase ensure the orderly termination of the system, safeguarding vital system information, and migrating data processed by the system to a new system.

SDLC principles extend to COTS (commercial off-the-shelf) software as well as open source software. It is important to recognize the stages of software releases. The alpha phase is the initial release of software for testing. Beta phase indicates that the software is feature complete and the focus is usability testing. A release candidate (RC) is a hybrid of a beta and a final release version. General availability or “go live” is when the software has been made commercially available and is in general distribution. Alpha, beta, and RCs should never be implemented in a production environment. Over the course of time, publishers may release updates and security patches. Updates generally include enhancements and new features. Updates should be thoroughly tested before release to a production environment. Even tested applications should have a rollback strategy just in case the unexpected happens. Live data should never be used in a test environment; instead, de-identified or dummy data should be used.

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted.

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. In 2013, OWASP rated injection flaws as the number-one software and database security issue. Injection is when untrusted data is sent to an interpreter as part of a command or query. Input and output validation minimizes injection vulnerabilities. Input validation is the process of validating all the input to an application before using it. This includes correct syntax, length, characters, and ranges. Output validation is the process of validating (and in some cases, masking) the output of a process before it is provided to the recipient.

Data at rest and in transit may require cryptographic protection. Three distinct goals are associated with cryptography: Data can be encrypted, which provides confidentiality. Data can be hashed, which provides integrity. Data can be digitally signed, which provides authenticity/nonrepudiation and integrity. Also, data can be encrypted and digitally signed, which provides for confidentiality, authentication, and integrity. Encryption is the conversion of plain text into what is known as cipher text using an algorithm called a cipher. Decryption, the inverse of encryption, is the process of turning cipher text back into readable plain text. Hashing is the process of creating a fixed-length value known as a fingerprint that represents the original text. A digital signature is a hash value (also known as a message digest) that has been encrypted with the sender's private key.

A key is a value that specifies what part of the cryptographic algorithm to apply, in what order, and what variables to input. The keyspace is a large set of random values that the algorithm chooses from when it needs to make a key. Symmetric key algorithms use a single secret key, which must be shared in advance and kept private by both the sender and the receiver. Asymmetric key cryptography, also known as public key cryptography, uses two different but mathematically related keys known as public and private keys. A digital certificate is used to associate a public key with an identity.

A Public Key Infrastructure (PKI) is used to create, distribute, manage, and revoke asymmetric keys. A Certification Authority (CA) issues and maintains digital certificates. A Registration Authority (RA) performs the administrative functions, including verifying the identity of users and organizations requesting a digital certificate, renewing certificates, and revoking certificates. Client nodes are interfaces for users, devices, and applications to access PKI functions, including the requesting of certificates and other keying material. They may include cryptographic modules, software, and procedures necessary to provide user access to the PKI.

Information Systems Acquisition, Development, and Maintenance (ISADM) policies include SDLC, Application Development, and Key Management.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. When is the best time to think about security when building an application?

   A. Build the application first and then add a layer of security.

   B. At inception.

   C. Start the application development phase, and when you reach the halfway point, you have enough of a basis to look at to decide where and how to set up the security elements.

   D. No security needs to be developed inside of the code itself. It will be handled at the operating system level.

2. Which of the following statements best describes the purpose of the systems development lifecycle (SDLC)?
   - A. The purpose of the SDLC is to provide a framework for system development efforts.
   - B. The purpose of the SDLC is to provide a standardized process for system development efforts.
   - C. The purpose of the SDLC is to assign responsibility.
   - D. All of the above.
3. In which phase of the SDLC is the need for a system expressed and the purpose of the system documented?
   - A. The initiation phase
   - B. The implementation phase
   - C. The operational phase
   - D. The disposal phase
4. During which phase of the SDLC is the system accepted?
   - A. The initiation phase
   - B. The implementation phase
   - C. The operational phase
   - D. The disposal phase
5. Which of the following statements is true?
   - A. Retrofitting security controls to an application system after implementation is normal; this is when security controls should be added.
   - B. Retrofitting security controls to an application system after implementation is sometimes necessary based on testing and assessment results.
   - C. Retrofitting security controls to an application system after implementation is always a bad idea.
   - D. Retrofitting security controls to an application system after implementation is not necessary because security is handled at the operating system level.
6. Which phase of software release indicates that the software is feature complete?
   - A. Alpha
   - B. Beta
   - C. Release candidate
   - D. General availability

7. Which phase of software release is the initial release of software for testing?

   A. Alpha

   B. Beta

   C. Release candidate

   D. General availability

8. Which of the following statements best describes the difference between a security patch and an update?

   A. Patches provide enhancements; updates fix security vulnerabilities.

   B. Patches should be tested; updates do not need to be tested.

   C. Patches fix security vulnerabilities; updates add features and functionality.

   D. Patches cost money; updates are free.

9. The purpose of a rollback strategy is to ______________.

   A. make backing up easier

   B. return to a previous stable state in case problems occur

   C. add functionality

   D. protect data

10. Which of the following statements is true?

    A. A test environment should always be the exact same as the live environment.

    B. A test environment should be as cheap as possible no matter what.

    C. A test environment should be as close to the live environment as possible.

    D. A test environment should include live data for true emulation of the real-world setup.

11. Which of the following statements best describes when dummy data should be used?

    A. Dummy data should be used in the production environment.

    B. Dummy data should be used in the testing environment.

    C. Dummy data should be used in both test and production environments.

    D. Dummy data should not be used in either test or production environments.

12. Which of the following terms best describes the process of removing information that would identify the source or subject?

    A. Detoxification

    B. Dumbing down

    C. Development

    D. De-identification

13. Which of the following terms best describes the open framework designed to help organizations implement a strategy for secure software development?

- **A.** OWASP
- **B.** SAMM
- **C.** NIST
- **D.** ISO

14. Which of the following statements best describes an injection attack?

- **A.** An injection attack occurs when untrusted data is sent to an interpreter as part of a command.
- **B.** An injection attack occurs when trusted data is sent to an interpreter as part of a query.
- **C.** An injection attack occurs when untrusted email is sent to a known third party.
- **D.** An injection attack occurs when untrusted data is encapsulated.

15. Input validation is the process of ___________.

- **A.** masking data
- **B.** verifying data syntax
- **C.** hashing input
- **D.** trusting data

16. Which of the following types of data changes as updates become available?

- **A.** Moving data
- **B.** Mobile data
- **C.** Dynamic data
- **D.** Delta data

17. The act of limiting the characters that can be entered in a web form is known as ___________.

- **A.** output validation
- **B.** input validation
- **C.** output testing
- **D.** input testing

18. Which statement best describes a distinguishing feature of cipher text?

- **A.** Cipher text is unreadable by a human.
- **B.** Cipher text is unreadable by a machine.
- **C.** Both A and B.
- **D.** Neither A nor B.

19. Which term best describes the process of transforming plain text to cipher text?

- **A.** Decryption
- **B.** Hashing
- **C.** Validating
- **D.** Encryption

20. Which of the following statements is true?

- **A.** Digital signatures guarantee confidentiality only.
- **B.** Digital signatures guarantee integrity only.
- **C.** Digital signatures guarantee integrity and nonrepudiation.
- **D.** Digital signatures guarantee nonrepudiation only.

21. Hashing is used to ensure message integrity by ____________.

- **A.** comparing hash values
- **B.** encrypting data
- **C.** encapsulating data
- **D.** comparing algorithms and keys

22. When unauthorized data modification occurs, which of the following tenets of security is directly being threatened?

- **A.** Confidentiality
- **B.** Integrity
- **C.** Availability
- **D.** Authentication

23. Which of the following statements about encryption is true?

- **A.** All encryption methods are equal: Just choose one and implement it.
- **B.** The security of the encryption relies on the key.
- **C.** Encryption is not needed for internal applications.
- **D.** Encryption guarantees integrity and availability, but not confidentiality.

24. Which of the following statements about a hash function is true?

- **A.** A hash function takes a variable-length input and turns it into a fixed-length output.
- **B.** A hash function takes a variable-length input and turns it into a variable-length output.
- **C.** A hash function takes a fixed-length input and turns it into a fixed-length output.
- **D.** A hash function takes a fixed-length input and turns it into a variable-length output.

25. Which of the following values represents the number of available values in a 256-bit keyspace?

A. 2×2^{256}

B. 2×256

C. 256^2

D. 2^{256}

26. Which of the following statements is *not* true about a symmetric key algorithm?

A. Only one key is used.

B. It is computationally efficient.

C. The key must be publicly known.

D. 3DES is widely used.

27. The contents of a __________ include the issuer, subject, valid dates, and public key.

A. digital document

B. digital identity

C. digital thumbprint

D. digital certificate

28. Two different but mathematically related keys are referred to as ___________.

A. public and private keys

B. secret keys

C. shared keys

D. symmetric keys

29. In cryptography, which of the following is *not* publicly available?

A. Algorithm

B. Public key

C. Digital certificate

D. Symmetric key

30. A hash value that has been encrypted with the sender's private key is known as a _________.

A. message digest

B. digital signature

C. digital certificate

D. cipher text

EXERCISES

EXERCISE 10.1: Building Security into Applications

1. Explain why security requirements should be considered at the beginning stages of a development project.
2. Who is responsible for ensuring that security requirements are defined?
3. In which phases of the SDLC should security be evaluated?

EXERCISE 10.2: Understanding Input Validation

1. Define input validation.
2. Describe the type of attack that is related to poor input validation.
3. In the following scenario, what should the input validation parameters be?

   A class registration web form requires that students enter their current year. The entry options are numbers from 1 to 4 that represent the following: freshmen=1, sophomores=2, juniors=3, and seniors=4.

EXERCISE 10.3: Researching Software Releases

1. Find an example of commercially available software that is available as either a beta version or a release candidate.
2. Find an example of open source software that is available as either an alpha, beta, or release candidate.
3. For each, does the publisher include a disclaimer or warning?

EXERCISE 10.4: Learning About Cryptography

1. Access the National Security Agency's CryptoKids website.
2. Play at least two of the games.
3. Explain what you learned.

EXERCISE 10.5: Understanding Updates and Systems Maintenance

1. Microsoft bundles feature and function updates and refers to them as "service packs." Locate a recently released service pack.
2. Does the service pack have a rollback option?
3. Explain why a rollback strategy is important when upgrading an operating system or application.

PROJECTS

PROJECT 10.1: Creating a Secure App

You have obtained financing to design a mobile device app that integrates with your school's student portal so that students can check easily check their grades from anywhere.

1. Create a list of security concerns. For each concern, indicate if the issue is related to confidentiality, integrity, availability (CIA), or any combination thereof.
2. Create a project plan using the SDLC framework as a guide. Describe your expectations for each phase. Be sure to include roles and responsibilities.
3. Research and recommend an independent security firm to test your application. Explain why you chose them.

PROJECT 10.2: Researching the Open Web Application Security Project (OWASP)

The OWASP Top Ten has become a must-read resource. Go to https://www.owasp.org and access the 2013 Top Ten Web Application report.

1. Read the entire report.
2. Write a memo addressed to Executive Management on why they should read the report. Include in your memo what OWASP means by "It's About Risks, Not Weaknesses" on page 20.
3. Write a second memo addressed to developers and programmers on why they should read the report. Include in your memo references to other OWASP resources that would be of value to them.

PROJECT 10.3: Researching Digital Certificates

You have been tasked with obtaining an extended validation SSL digital certificate for an online shopping portal.

1. Research and choose an issuing CA. Explain why you chose the specific CA.
2. Describe the process and requirements for obtaining a digital certificate.
3. Who in the organization should be tasked with installing the certificate and why?

Case Study

On Thursday January 3, 2013, Microsoft issued the following Security Advisory (2798897):

"Fraudulent Digital Certificates Could Allow Spoofing

"Microsoft is aware of active attacks using one fraudulent digital certificate issued by TURKTRUST Inc., which is a CA present in the Trusted Root Certification Authorities Store. This fraudulent certificate could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks. This issue affects all supported releases of Microsoft Windows.

"TURKTRUST Inc. incorrectly created two subsidiary CAs (*.EGO.GOV.TR and e-islem.kktcmerkezbankasi.org). The *.EGO.GOV.TR subsidiary CA was then used to issue a fraudulent digital certificate to *.google.com. This fraudulent certificate could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against several Google web properties.

"To help protect customers from the fraudulent use of this digital certificate, Microsoft is updating the Certificate Trust List (CTL) and is providing an update for all supported releases of Microsoft Windows that removes the trust of certificates that are causing this issue.

For systems using the automatic updater of revoked certificates (see Microsoft Knowledge Base Article 2677070 for details), including Windows 8, Windows RT, Windows Server 2012, and devices running Windows Phone 8, no action is needed as these systems will be automatically protected.

For Windows XP and Windows Server 2003 customers or customers who choose not to install the automatic updater of revoked certificates, Microsoft recommends that the 2798897 update be applied immediately using update management software, by checking for updates using the Microsoft Update service, or by downloading and applying the update manually."

1. Who is TURKTRUST?
2. Explain what happened and why this is a potentially dangerous situation.
3. Research this event. Did any other organizations issue advisories?

References

Regulations Cited

16 CFR Part 314: Standards for Safeguarding Customer Information; Final Rule, Federal Register, accessed 05/2013, http://ithandbook.ffiec.gov/media/resources/3337/joisafeguard_customer_info_final_rule.pdf.

"201 Cmr 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth," official website of the Office of Consumer Affairs & Business Regulation (OCABR), accessed 05/2013, www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

"HIPAA Security Rule," official website of the Department of Health and Human Services, accessed 05/2013, www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

State of Nevada, "Chapter 603A—Security of Personal Information," accessed 08/2013, www.leg.state.nv.us/NRS/NRS-603A.html.

State of Washington, "HB 2574, An Act Relating to Securing Personal Information Accessible Through the Internet," accessed 08/2013, apps.leg.wa.gov/documents/billdocs/2007-08/Pdf/Bills/.../2574.pdf.

Other References

"Certificate," Microsoft Technet, accessed 08/2013, http://technet.microsoft.com/en-us/library/cc700805.aspx.

"Encryption Explained," Indiana University Information Security & Policy, accessed 08/2013, http://protect.iu.edu/cybersecurity/data/encryption.

Microsoft Corp. "Fraudulent Digital Certificates Could Allow Spoofing," Microsoft Security Advisory (2798897), January 3, 2013, accessed 08/2013, http://technet.microsoft.com/en-us/security/advisory/2798897.

Kak, Avi, "Lecture 15: Hashing for Message Authentication, Lecture Notes on Computer and Network Security,"PurdueUniversity,April28,2013.https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture15.pdf

"Open SAMM: Software Assurance Maturity Model Software Assurance Maturity Model," OWASP Wiki, Creative Commons (CC) Attribution Share-Alike 3.0 License, accessed 08/2013, www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model.

"OpenSAMM: Software Assurance Maturity Model," accessed 08/2013, www.opensamm.org/.

"Public-key Cryptography" (redirected from Asymmetric key Algorithm), Wikipedia, accessed 08/2013, http://en.wikipedia.org/wiki/Asymmetric_key_algorithm.

"RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP," June 2013, Internet Engineering Task Force, accessed 08/2013, http://tools.ietf.org/html/rfc6960.

"RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," May 2008, Internet Engineering Task Force, accessed 08/2013, http://tools.ietf.org/html/rfc5280.

"Top 10 2013: The Ten Most Critical Web Application Security Risks," The OWASP Foundation, Creative Commons (CC) Attribution Share-Alike 3.0 License, accessed 08/2013, www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

"The Case for Email Encryption, Required by Law," ZixCorp white paper, accessed 08/2013, www.zixcorp.com/.../case.../Case_for_Email_Encry_Required_by_Law.....

Turner, P., W. Polk, and E. Barker. "Preparing for and Responding to Certification Authority Compromise and Fraudulent Certificate Issuance," NIST, ITL Bulletin, July 2012.

Chapter 11

Information Security Incident Management

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Prepare for an information security incident.
- Identify an information security incident.
- Recognize the stages in incident management.
- Properly document an information security incident.
- Understand federal and state data breach notification requirements.
- Consider an incident from the perspective of the victim.
- Create policies related to information security incident management.

Incidents happen. Security-related incidents have become not only more numerous and diverse but also more damaging and disruptive. A single incident can cause the demise of an entire organization. In general terms, incident management is defined as a predicable response to damaging situations. It is vital that organizations have the practiced capability to respond quickly, minimize harm, comply with breach-related state laws and federal regulations, and maintain their composure in the face of an unsettling and unpleasant experience.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 16 of ISO 27002:2013: Information Security Incident Management focuses on ensuring a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Corresponding NIST guidance is provided in the following documents:

- SP 800-61: Computer Security Incident Handling Guide
- SP 800-66: Guide to Integrating Forensic Techniques into Incident Response

Organizational Incident Response

Incidents drain resources, can be very expensive, and divert attention from the business of doing business. Keeping the number of incidents as low as possible should be an organization priority. That means as much as possible identifying and remediating weaknesses and vulnerabilities before they are exploited. As we discussed in Chapter 4, "Governance and Risk Management," a sound approach to improving an organizational security posture and preventing incidents is to conduct periodic risk assessments of systems and applications. These assessments should determine what risks are posed by combinations of threats, threat sources, and vulnerabilities. Risks can be mitigated, transferred, or avoided until a reasonable overall level of acceptable risk is reached. That said, it is important to realize that users will make mistakes, external events may be out of an organization's control, and malicious intruders are motivated. Unfortunately, even the best prevention strategy isn't always enough, which is why preparation is key.

Incident preparedness includes having policies, strategies, plans, and procedures. Organizations should create written guidelines, have supporting documentation prepared, train personnel, and engage in mock exercises. An actual incident is not the time to learn. Incident handlers must act quickly and make far-reaching decisions—often while dealing with uncertainty and incomplete information. They are under a great deal of stress. The more prepared they are, the better the chance that sound decisions will be made.

The benefits of having a practiced incident response capability include the following:

- Calm and systematic response
- Minimization of loss or damage
- Protection of affected parties
- Compliance with laws and regulations
- Preservation of evidence
- Integration of lessons learned
- Lower future risk and exposure

FYI: United States Computer Emergency Readiness Team (US-CERT)

US-CERT is the 24-hour operational arm of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC). US-CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities.

US-CERT also distributes vulnerability and threat information through its National Cyber Awareness System (NCAS). There are four mailing lists that anyone can subscribe to:

- **Alerts**—Timely information about current security issues, vulnerabilities, and exploits.
- **Bulletins**—Weekly summaries of new vulnerabilities. Patch information is provided when available.
- **Tips**—Advice about common security issues for the general public.
- **Current Activity**—Up-to-date information about high-impact types of security activity affecting the community at large.

To subscribe, visit https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.

What Is an Incident?

An ***information security incident*** is an adverse event that threatens business security and/or disrupts service. Sometimes confused with a disaster, an information security incident is related to loss of confidentiality, integrity, or availability (CIA) (whereas a disaster is an event that results in widespread damage or destruction, loss of life, or drastic change to the environment). Examples of incidents include exposure of or modification of legally protected data, unauthorized access to intellectual property, or disruption of internal or external services. The starting point of incident management is to create an organization-specific definition of the term *incident* so that the scope of the term is clear. Declaration of an incident should trigger a mandatory response process. The definition and criteria should be codified in policy. Incident management extends to third-party environments. As we discussed in Chapter 8, "Communications and Operations Security," business partners and vendors should be contractually obligated to notify the organization if there is an actual or suspected incident.

In Practice

Incident Definition Policy

Synopsis: To define organizational criteria pertaining to an information security incident.

Policy Statement:

- An information security incident is an event that has the potential to adversely impact the company, our clients, our business partners, and/or the public-at-large.

- An information security incident is defined as:
    - Actual or suspected unauthorized access to, compromise of, acquisition of, or modification of protected client or employee data, including but not limited to:
        - personal identification numbers, such as social security numbers (SSNs), passport numbers, driver's license numbers
        - financial account or credit card information, including account numbers, card numbers, expiration dates, cardholder name, and service codes
        - healthcare/medical information
    - Actual or suspected event that has the capacity to disrupt the services provided to our clients.
    - Actual or suspected unauthorized access to, compromise of, acquisition of, or modification of company intellectual property.
    - Actual or suspected event that has the capacity to disrupt the company's ability to provide internal computing and network services.
    - Actual or suspected event that is in violation of legal or statutory requirements.
    - Actual or suspected event not defined above that warrants incident classification as determined by management.
- All employees, contractors, consultants, vendors, and business partners are required to report known or suspected information security incidents.
- This policy applies equally to internal and third-party incidents.

Although any number of events could result in an incident, a core group of attacks or situations are most common. Every organization should understand and be prepared to respond to intentional unauthorized access, distributed denial of service (DDoS) attacks, malicious code (malware), and inappropriate usage.

Intentional Unauthorized Access or Use

An intentional unauthorized access incident occurs when an insider or intruder gains logical or physical access without permission to a network, system, application, data, or other resource. Intentional unauthorized access is typically gained through the exploitation of operating system or application vulnerabilities using malware or other targeted exploit, the acquisition of usernames and passwords, the physical acquisition of a device, or social engineering. Attackers may acquire limited access through one vector and use that access to move to the next level.

Denial of Service (DoS) Attacks

A ***denial of service (DoS) attack*** is an attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources or in some way obstructs or overloads the communication channel. This attack may be directed at the organization or may be consuming resources as an unauthorized participant in a DoS attack. DoS attacks have become an increasingly severe threat, and the lack of availability of computing and network services now translates to significant disruption and major financial loss.

NOTE

Refer to Chapter 8 for a description of DOS attacks.

FYI: October 2013: Thirteen Indicted for DDoS Attacks

On October 3, 2013, a grand jury in U.S. District Court in Alexandria, Virginia indicted 13 men suspected of launching distributed denial of service (DDoS) attacks against the websites of major companies, including Visa, MasterCard, Bank of America, the Motion Picture Association of America (MPAA), the Recording Industry Association of America (RIAA), and the United States Copyright Office of the Library of Congress. All were charged with one count of conspiracy to intentionally cause damage to a protected computer.

The indictment charged that the men, together with others known and unknown to the Grand Jury, participated in a worldwide conspiracy as part of the online group Anonymous in a campaign dubbed "OPERATION PAYBACK" to engage in a coordinated series of cyber attacks.

The defendants were accused of planning and executing a coordinated series of cyber attacks against victim websites by flooding those websites with a huge volume of irrelevant Internet traffic with the intent to make the resources on the websites unavailable to customers and users of those websites. This method of online attack is known as a DDoS attack.

To attack these sites, the group used and, in some cases, "publicized and distributed to other Anonymous members," a Low Orbit Ion Cannon—an open source network stress tool that can double as a program that sends large chunks of traffic to overwhelm web servers, the indictment said.

Malware

Malware has become the tool of choice for cybercriminals, hackers, and hacktivists. ***Malware*** (malicious software) refers to code that is covertly inserted into another program with the intent of gaining unauthorized access, obtaining confidential information, disrupting operations, destroying data, or in some manner compromising the security or integrity of the victim's data or system. Malware is designed to function without the system's user knowledge There are multiple categories of malware, including virus, worm, Trojans, bots, ransomware, rootkits, and spyware/adware. Suspicion of or evidence of malware infection should be considered an incident. Malware that has been successfully quarantined by antivirus software should not be considered an incident.

NOTE

Refer to Chapter 8 for an extensive discussion of malware.

Inappropriate Usage

An inappropriate usage incident occurs when an authorized user performs actions that violate internal policy, agreement, law, or regulation. Inappropriate usage can be internal facing, such as accessing data when there is clearly not a "need to know." An example would be when an employee or contractor views a patient's medical records or a bank customer's financial records purely for curiosity's sake, or when the employee or contractor shares information with unauthorized users. Conversely, the perpetrator can be an insider and the victim can be a third party (for example, the downloading of music or video in violation of copyright laws).

Incident Severity Levels

Not all incidents are equal in severity. Included in the incident definition should be severity levels based on the operational, reputational, and legal impact to the organization. Corresponding to the level should be required response times as well as minimum standards for internal notification. Table 11.1 illustrates this concept.

TABLE 11.1 Incident Severity Level Matrix

An information security incident is any adverse event whereby some aspect of an information system or information itself is threatened. Incidents are classified by severity relative to the impact they have on an organization. Each level has a maximum response time and minimum internal notification requirements.	
Severity Level = 1	
Explanation	Level I incidents are defined as those that could cause significant harm to the business, customers, or the public and/or are in violation of corporate law, regulation, or contractual obligation.
Required Response Time	Immediate.
Required Internal Notification	Chief Executive Officer. Chief Operating Officer. Legal counsel. Chief Information Security Officer. Designated incident handler.
Examples	Compromise or suspected compromise of protected customer information. Theft or loss of any device or media on any device that contains legally protected information. A denial of service attack. Identified connection to "command and control" sites. Compromise or suspected compromise of any company website or web presence. Notification by a business partner or vendor of a compromise or potential compromise of a customer or customer-related information. Any act that is in direct violation of local, state, or federal law or regulation.

Severity Level = 2	
Explanation	Level 2 incidents are defined as compromise of or unauthorized access to noncritical systems or information; detection of a precursor to a focused attack; a believed threat of an imminent attack; or any act that is a potential violation of law, regulation, or contractual obligation.
Required Response Time	Within four hours.
Required Internal Notification	Chief Operating Officer. Legal counsel. Chief Information Security Officer. Designated incident handler.
Examples	Inappropriate access to legally protected or proprietary information. Malware detected on multiple systems. Warning signs and/or reconnaissance detected related to a potential exploit. Notification from a third party of an imminent attack.
Severity Level = 3	
Explanation	Level 3 incidents are defined as situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel. There is no evidence or suspicion of harm to customer or proprietary information, processes, or services.
Required Response Time	Within 24 hours.
Required Internal Notification	Chief Information Security Officer. Designated incident handler.
Examples	Malware detected and/or suspected on a workstation or device, with no external connections identified. User access to content or sites restricted by policy. User's excessive use of bandwidth or resources.

How Are Incidents Reported?

Incident reporting is best accomplished by implementing simple, easy-to-use mechanisms that can be used by all employees to report the discovery of an incident. Employees should be required to report all actual and suspected incidents. They should not be expected to assign a severity level, because the person who discovers an incident may not have the skill, knowledge, or training to properly assess the impact of the situation.

People frequently fail to report potential incidents because they are afraid of being wrong and looking foolish, they do not want to be seen as a complainer or whistleblower, or they simply don't care enough and would prefer not to get involved. These objections must be countered by encouragement from management. Employees must be assured that even if they were to report a perceived incident that ended up being a false positive, they would not be ridiculed or met with annoyance. On the contrary, their willingness to get involved for the greater good of the company is exactly the type of behavior the company needs! They should be supported for their efforts and made to feel valued and appreciated for doing the right thing.

In Practice

Information Security Incident Classification Policy

Synopsis: Classify incidents by severity and assigned response and notification requirements.

Policy Statement:

- Incidents are to be classified by severity relative to the impact they have on an organization. If there is ever a question as to which level is appropriate, the company must err on the side of caution and assign the higher severity level.
- Level 1 incidents are defined as those that could cause significant harm to the business, customers, or the public and/or are in violation of corporate law, regulation, or contractual obligation:
  - Level 1 incidents must be responded to immediately upon report.
  - The Chief Executive Officer, Chief Operating Officer, legal counsel, and Chief Information Security Officer must be informed of Level 1 incidents.
- Level 2 incidents are defined as a compromise of or unauthorized access to noncritical systems or information; detection of a precursor to a focused attack; a believed threat of an imminent attack; or any act that is a potential violation of law, regulation, or contractual obligation:
  - Level 2 incidents must be responded to within four hours.
  - The Chief Operating Officer, legal counsel, and Chief Information Security Officer must be informed of Level 2 incidents.
- Level 3 incidents are defined as situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel. There is no evidence or suspicion of harm to customer or proprietary information, processes, or services:
  - Level 3 incidents must be responded to within 24 business hours.
  - The Information Security Officer must be informed of Level 3 incidents.

What Is an Incident Response Program?

An ***incident response program*** is composed of policies, plans, procedures, and people. Incident response policies codify management directives. Incident response plans (IRPs) provide a well-defined, consistent, and organized approach for handling internal incidents as well as taking appropriate action when an external incident is traced back to the organization. Incident response procedures are detailed steps needed to implement the plan.

An ***incident response plan (IRP)*** is a roadmap, guidance, and instructions related to preparation, detection and analysis, initial response, containment, eradication and recovery, notification closure and post-incident activity, and documentation and evidence-handling requirements. Although described in a linear fashion, these activities often happen in parallel:

- ***Preparation*** includes developing internal incident response capabilities, establishing external contracts and relationships, defining legal and regulatory requirements, training personnel, and testing plans and procedures.
- ***Detection and investigation*** include establishing processes and a knowledge base to accurately detect and assess precursors and indicators. A ***precursor*** is a signal or warning that an incident may occur in the future. An ***indicator*** is substantive or corroborating evidence that an incident may have occurred or may be occurring now. Indicators are sometimes referred to as IOCs (indicators of compromise).
- ***Initial response*** include incident declaration, internal notification, activation of an incident response team, and/or designated incident handlers, and prioritization of response activities.
- ***Containment*** includes taking the steps necessary to prevent the incident from spreading, and as much as possible limit the potential for further damage.
- ***Eradication and recovery*** include the elimination of the components of the incident (for example, malicious code, compromised passwords), addressing the vulnerabilities related to the exploit or compromise, and restoring normal operations.
- ***Notification*** includes the steps taken to notify state and federal agencies, affected parties, victims, and the public-at-large.
- ***Closure and post-incident activity*** include incident recap, information sharing, documentation of "lessons learned," plan and procedure updates, and policy updates and risk reviews, as applicable.
- ***Documentation and evidence-handling requirements*** include the recording of facts, observations, participants, actions taken, forensic analysis, and evidence chain of custody. Although the primary reason for gathering evidence during an incident is to resolve the incident, it may also be needed for subsequent risk assessments, notifications, and legal proceedings.

In Practice

Information Security Incident Response Program Policy

Synopsis: To ensure that information security incidents are responded to, managed, and reported in a consistent and effective manner.

Policy Statement:

- An incident response plan (IRP) will be maintained to ensure that information security incidents are responded to, managed, and reported in a consistent and effective manner.
- The Office of Information Security is responsible for the establishment and maintenance of an IRP.
- The IRP will, at a minimum, include instructions, procedures, and guidance related to:
    - Preparation
    - Detection and investigation
    - Initial response
    - Containment
    - Eradication and recovery
    - Notification
    - Closure and post-incident activity
    - Documentation and evidence handling
- In accordance with the Information Security Incident Personnel Policy, the IRP will further define personnel roles and responsibilities, including but not limited to incident response coordinators, designated incident handlers, and incident response team members.
- All employees, contractors, consultants, and vendors will receive incident response training appropriate to their role.
- The IRP must be annually authorized by the Board of Directors.

Key Incident Management Personnel

Key incident management personnel include incident response coordinators, designated incident handlers, incident response team members, and external advisors. In various organizations, they may have different titles but the roles are essentially the same.

The ***incident response coordinator (IRC)*** is the central point of contact for all incidents. Incident reports are directed to the IRC. The IRC verifies and logs the incident. Based on predefined criteria, the IRC notifies appropriate personnel, including the designated incident handler (DIH). The IRC is a member of the incident response team (IRT) and is responsible for maintaining all non-evidence-based incident-related documentation.

Designated incident handlers (DIHs) are senior-level personnel who have the crisis management and communication skills, experience, knowledge, and stamina to manage an incident. DIHs are responsible for three critical tasks: incident declaration, liaison with executive management, and managing the incident response team (IRT).

The ***incident response team (IRT)*** is a carefully selected and well-trained team of professionals that provides services throughout the incident lifecycle. Depending on the size of the organization, there may be a single team or multiple teams, each with their own specialty. The IRT members generally represent a cross-section of functional areas, including senior management, information security, information technology (IT), operations, legal, compliance, HR, public affairs and media relations, customer service, and physical security. Some members may be expected to participate in every response effort, whereas others (such as compliance) may restrict involvement to relevant events. The team as directed by the DIH is responsible for further analysis, evidence handling and documentation, containment, eradication and recovery, notification (as required), and post-incident activities.

Tasks assigned to the IRT include but are not limited to the following:

- Overall management of the incident
- Triage and impact analysis to determine the extent of the situation
- Development and implementation of containment and eradication strategies
- Compliance with government and/or other regulations
- Communication and follow-up with affected parties and/or individuals
- Communication and follow-up with other external parties, including the Board of Directors, business partners, government regulators (including federal, state, and other administrators), law enforcement, representatives of the media, and so on, as needed
- Root cause analysis and lessons learned
- Revision of policies/procedures necessary to prevent any recurrence of the incident

Figure 11.1 illustrates the incident response roles and responsibilities.

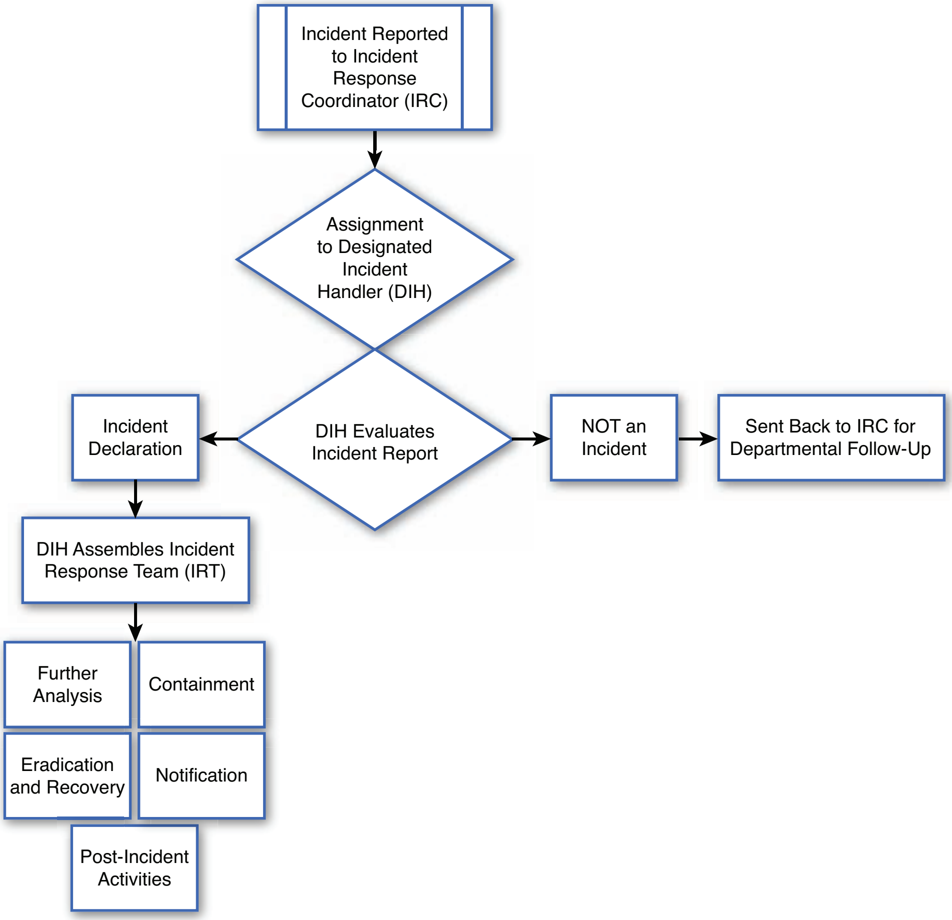

Incident Reported to Incident Response Coordinator (IRC)
Assignment to Designated Incident Handler (DIH)
Incident Declaration
DIH Evaluates Incident Report
NOT an Incident
Sent Back to IRC for Departmental Follow-Up
DIH Assembles Incident Response Team (IRT)
Further Analysis
Containment
Eradication and Recovery
Notification
Post-Incident Activities

FIGURE 11.1 Incident response roles and responsibilities.

Communicating Incidents

Throughout the incident lifecycle, there is frequently the need to communicate with outside parties, including law enforcement, insurance companies, legal counsel, forensic specialists, the media, vendors, external victims, and other IRTs. Having up-to-date contact lists is essential. Because such communications often need to occur quickly, organizations should predetermine communication guidelines and preapprove external resources so that only the appropriate information is shared with the outside parties.

Incident Response Training and Exercises

Establishing a robust response capability ensures that the organization is prepared to respond to an incident swiftly and effectively. Responders should receive training specific to their individual and collective responsibilities. Recurring tests, drills, and challenging incident response exercises can make a huge difference in responder ability. Knowing what is expected decreases the pressure on the responders and reduces errors. It should be stressed that the objective of incident response exercises isn't to get an "A" but rather to honestly evaluate the plan and procedures, to identify missing resources, and to learn to work together as a team.

In Practice

Incident Response Authority Policy

Synopsis: To vest authority in those charged with responding to and/or managing an information security incident.

Policy Statement:

- The Chief Information Security Officer has the authority to appoint IRC, DIHs, and IRT members:
  - All responders must receive training commensurate with their role and responsibilities.
  - All responders must participate in recurring drills and exercises.
- During a security incident, as well as during drills and exercises, incident management and incident response–related duties supersede normal duties.
- The Chief Operating Office and/or legal counsel have the authority to notify law enforcement or regulatory officials.
- The Chief Operating Officer, Board of Directors, and/or legal counsel have the authority to engage outside personnel, including but not limited to forensic investigators, experts in related fields (such as security, technology, and compliance), and specialized legal counsel.

What Happened? Investigation and Evidence Handling

The primary reason for gathering evidence is to figure out "what happened" in order to contain and resolve the incident as quickly as possible. As an incident responder, it is easy to get caught up in the moment. It may not be apparent that careful evidence acquisition, handling, and documentation are important or even necessary. Consider the scenario of a workstation malware infection. The first impression may be that the malware download was inadvertent. This could be true or perhaps it was the work of a malicious insider or careless business vendor. Until you have the facts, you just don't know. Regardless of the source, if the malware infection resulted in a compromise of legally protected information, the company could be a target of a negligence lawsuit or regulatory action, in which case evidence of how the infection was contained and eradicated could be used to support the company's position. Because there are so many variables, by default, data handlers should treat every investigation as if it would lead to a court case.

Documenting Incidents

The initial documentation should create an incident profile. The profile should include the following:

- How was the incident detected?
- What is the scenario for the incident?
- What time did the incident occur?
- Who or what reported the incident?
- Who are the contacts for involved personnel?
- A brief description of the incident.
- Snapshots of all on-scene conditions.

All ongoing incident response–related activity should be logged and time stamped. In addition to actions taken, the log should include decisions, record of contact (internal and external resources), and recommendations.

Documentation specific to computer-related activity should be kept separate from general documentation due to the confidential nature of what is being performed and/or found. All documentation should be sequential and time/date stamped, and should include exact commands entered into systems, results of commands, actions taken (for example, logging on, disabling accounts, applying router filters) as well as observations about the system and/or incident. Documentation should occur as the incident is being handled, not after.

Incident documentation should not be shared with anyone outside the team without the express permission of the DIH or executive management. If there is any expectation that the network has been compromised, documentation should not be saved on a network-connected device.

Working with Law Enforcement

Depending on the nature of the situation, it may be necessary to contact local, state, or federal law enforcement. The decision to do so should be discussed with legal counsel. It is important to recognize that the primary mission of law enforcement is to identify the perpetrators and build a case. There may be times when the law enforcement agency requests that the incident or attack continue while they work to gather evidence. Although this objective appears to be at odds with the organizational objective to contain the incident, it is sometimes the best course of action. The IRT should become acquainted with applicable law enforcement representatives before an incident occurs to discuss the types of incidents that should be reported to them, who to contact, what evidence should be collected, and how it should be collected.

If the decision is made to contact law enforcement, it is important to do so as early in the response lifecycle as possible while the trail is still hot. On a federal level, both the Secret Service and the Federal Bureau of Investigation (FBI) investigate cyber incidents. The Secret Service's investigative responsibilities extend to crimes that involve financial institution fraud, computer and telecommunications fraud, identity theft, access device fraud (for example, ATM or point of sale systems), electronic funds transfers, money laundering, corporate espionage, computer system intrusion, and Internet-related child pornography and exploitation. The FBI's investigation responsibilities include cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. If the missions appear to overlap, it is because they do. Generally, it is best to reach out to the local Secret Service or FBI office and let them determine jurisdiction.

FYI: Arrested by the FBI for Hacking into Multiple Computer Networks

From 2008 to 2011, Andrew James Miller remotely hacked into a variety of computers located in Massachusetts and elsewhere and, in some instances, surreptitiously installed "backdoors" into those computers. These backdoors were designed to provide future administrator-level (or "root") access to the compromised computers. Miller obtained log-in credentials to the compromised computers. He and his co-conspirators then sold access to these backdoors, as well as other log-in credentials. The access sold by Miller and his co-conspirators allowed unauthorized people to access various commercial, education, and government computer networks.

On August 27, 2013, Miller pleaded guilty before U.S. District of Massachusetts Judge Mark Wolf to one count of conspiracy and two counts of computer intrusion. The maximum penalty for conspiracy is five years in prison. One of the computer intrusion counts carries a maximum penalty of five years in prison and the other, involving intentional damage to a private computer, carries a maximum penalty of ten years in prison. The investigation was conducted by the FBI's Boston Field Division.

Understanding Forensic Analysis

Forensics is the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information. Forensic tools and techniques are often used to find the root cause of an incident or to uncover facts. In addition to reconstructing security incidents, digital forensic techniques can be used for investigating crimes and internal policy violations, troubleshooting operational problems, and recovering from accidental system damage.

As described in NIST Special Publication 800-87, the process for performing digital forensics includes collection, examination, analysis, and reporting:

- **Collection**—The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data. Collection is typically performed in a timely manner because of the likelihood of losing dynamic data such as current network connections, as well as losing data from battery-powered devices.

- **Examination**—Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.
- **Analysis**—The next phase of the process is to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
- **Reporting**—The final phase is reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed, and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation.

Incident handlers performing forensic tasks need to have a reasonably comprehensive knowledge of forensic principles, guidelines, procedures, tools, and techniques, as well as anti-forensic tools and techniques that could conceal or destroy data. It is also beneficial for incident handlers to have expertise in information security and specific technical subjects, such as the most commonly used operating systems, file systems, applications, and network protocols within the organization. Having this type of knowledge facilitates faster and more effective responses to incidents. Incident handlers also need a general, broad understanding of systems and networks so that they can determine quickly which teams and individuals are well suited to providing technical expertise for particular forensic efforts, such as examining and analyzing data for an uncommon application.

FYI: CCFP—Certified Cyber Forensics Professional

The CCFP certication is offered by (ISC)^2. According to the ISC, “the Certified Cyber Forensics Professional (CCFP) credential indicates expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete, and reliable digital evidence admissible to a court of law. It also indicates the ability to apply forensics to other information security disciplines, such as e-discovery, malware analysis, or incident response.” To learn more, go to https://www.isc2.org/ccfp/.

All (ISC)^2 certifications are accredited by the American National Standards Institute (ANSI) to be in compliance with the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 17024 Standards.

Understanding Chain of Custody

Chain of custody applies to physical, digital, and forensic evidence. Evidentiary ***chain of custody*** is used to prove that evidence has not be altered from the time it was collected through production in court. This means that the moment evidence is collected, every transfer of evidence from person to person must be documented and that it must be provable that nobody else could have accessed that evidence. In the case of legal action, the chain of custody documentation will be available to opposing counsel through the information discovery process and may become public. Confidential information should only be included in the document if absolutely necessary.

To maintain an evidentiary chain, a detailed log should be maintained that includes the following information:

- Where and when (date and time) evidence was discovered
- Identifying information such as the location, serial number, model number, hostname, media access control (MAC) address, and/or IP address
- Name, title, and phone number of each person who discovered, collected, handled, or examined the evidence
- Where evidence was stored/secured and during what time period
- If the evidence has changed custody, how and when the transfer occurred (include shipping numbers, and so on).

The relevant person should sign and date each entry in the record.

Storing and Retaining Evidence

It is not unusual to retain all evidence for months or years after the incident ends. Evidence, logs, and data associated with the incident should be placed in tamper-resistant containers, grouped together, and put in a limited-access location. Only incident investigators, executive management, and legal counsel should have access to the storage facility. If and when evidence is turned over to law enforcement, an itemized inventory of all the items should be created and verified with the law enforcement representative. The law enforcement representative should sign and date the inventory list.

Evidence needs to be retained until all legal actions have been completed. Legal action could be civil, criminal, regulatory, or personnel related. Evidence-retention parameters should be documented in policy. Retention schedules should include the following categories: internal only, civil, criminal, regulatory, personnel-related incident, and to-be-determined (TBD). When categorization is in doubt, legal counsel should be consulted. If there is an organizational retention policy, a notation should be included that evidence-retention schedules (if longer) supersede operational or regulatory retention requirements.

In Practice

Evidence Handling and Use Policy

Synopsis: To ensure that evidence is handled in accordance with legal requirements.

Policy Statement:

- All evidence, logs, and data associated with the incident must be handled as follows:
    - All evidence, logs, and data associated with the incident must be labeled.
    - All evidence, logs, and data associated with the incident should be placed in tamper-resistant containers, grouped together, and put in a limited access location.
- All evidence handling must be recorded on a chain of custody.
- Unless otherwise instructed by legal counsel or law enforcement officials, all internal digital evidence should be handled in accordance with the procedures described in “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition” from the United States Department of Justice, National Institute of Justice (April 2008). If not possible, deviations must be noted.
- Unless otherwise instructed by legal counsel or law enforcement officials, subsequent internal forensic investigation and analysis should follow the guidelines provided in “Forensic Examination of Digital Evidence: A Guide for Law Enforcement” from the United States Department of Justice, National Institute of Justice (April 2004). If not possible, deviations must be noted.
- Executive management and the DIH have the authority to engage outside expertise for forensic evidence handling investigation and analysis.
- Exceptions to this policy can only be authorized by legal counsel.

Data Breach Notification Requirements

A component of incident management is to understand, evaluate, and be prepared to comply with the legal responsibility to notify affected parties. Most states have some form of data breach notification laws. Federal regulations, including but not limited to the Gramm-Leach-Bliley Act (GLBA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Federal Information Security Management Act (FISMA), and the Federal Educational Rights and Privacy Act (FERPA), all address the protection of personally identifiable information (PII; also referred to as non-public personal information, or NPPI) and may potentially apply in an event of an incident.

A data breach is widely defined as an incident that results in compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or unauthorized use or loss of control of legally protected PII, including the following:

- Any information that can be used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother's maiden name, or biometric records.
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- Information that is standing alone is not generally considered personally identifiable, because many people share the same trait, such as first or last name, country, state, ZIP Code, age (without birthdate), gender, race, or job position. However, multiple pieces of information, none of which alone may be considered personally identifiable, may uniquely identify a person when brought together.

Incidents resulting in unauthorized access to PII are taken seriously, as the information can be used by criminals to make false identification documents (including drivers' licenses, passports, and insurance certificates), make fraudulent purchases and insurance claims, obtain loans or establish lines of credit, and apply for government and military benefits.

As we will discuss, the laws vary and sometimes even conflict in their requirements regarding the right of the individual to be notified, the manner in which they must be notified, and the information to be provided. What is consistent, however, is that notification requirements apply regardless of whether an organization stores and manages its data directly or through a third party, such as a cloud service provider.

FYI: Chronology of Significant Data Breaches by Year

Year	Company	# Records	Information Disclosed
2005	CardSystems	40,000,000	Credit and debit card data
2006	Veterans Administration	26,500,000	Personal information
2007	TJX Companies	94,000,000	Credit and debit card data
2008	Chilean Ministry of Education	6,000,000	Personal information
2009	Heartland Payment Systems	130,000,000	Credit and debit card data
2010	Honda Motor Co.	4,900,000	Personal information
2011	Sony Corporation	77,000,000	Personal information
2012	Zappos	24,000,000	Personal information
2013	Living Social	50,000,000	Personal information

Information provided by DataLossDB (www.datalossdb.org).

Is There a Federal Breach Notification Law?

The short answer is, there is not. Consumer information breach notification requirements have historically been determined at the state level. There are, however, federal statutes and regulations that require certain regulated sectors (such as healthcare, financial, and investment) to protect certain types of personal information, implement information security programs, and provide notification of security breaches. In addition, federal departments and agencies are obligated by memorandum to provide breach notification. The Veterans Administration is the only agency with its own law governing information security and privacy breaches.

GLBA Financial Institution Customer Information

Section 501(b) of the GLBA and FIL-27-2005 Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice require that a financial institution provide a notice to its customers whenever it becomes aware of an incident of unauthorized access to customer information and, at the conclusion of a reasonable investigation, determines that misuse of the information has occurred or it is reasonably possible that misuse will occur.

Customer notice should be given in a clear and conspicuous manner. The notice should include the following items:

- Description of the incident
- Type of information subject to unauthorized access
- Measures taken by the institution to protect customers from further unauthorized access
- Telephone number that customers can call for information and assistance
- A reminder to customers to remain vigilant over the next 12 to 24 months and to report suspected identity theft incidents to the institution

The guidance encourages financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

Customer notices are required to be delivered in a manner designed to ensure that a customer can reasonably be expected to receive them. For example, the institution may choose to contact all customers affected by telephone, by mail, or by electronic mail (for those customers for whom it has a valid email address and who have agreed to receive communications electronically).

Financial institutions must notify their primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of non-public customer information. Consistent with the agencies' Suspicious Activity Report (SAR) regulations, institutions must file a timely SAR. In situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, institutions must promptly notify appropriate law enforcement authorities. Reference Chapter 12, "Business Continuity Management," for a further discussion of financial institution–related security incidents.

HIPAA/HITECH Personal Healthcare Information (PHI)

The HITECH Act requires that covered entities notify affected individuals when they discover that their unsecured PHI has been, or is reasonably believed to have been, breached—even if the breach occurs through or by a business associate. A breach is defined as "impermissible acquisition, access, or use or disclosure of unsecured PHI… unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised."

The notification must be made without unreasonable delay and no later than 60 days after the discovery of the breach. The covered entity must also provide notice to "prominent media outlets" if the breach affects more than 500 individuals in a state or jurisdiction. The notice must include the following information:

- A description of the breach, including the date of the breach and date of discovery
- The type of PHI involved (such as full name, SSN, date of birth, home address, or account number)
- Steps individuals should take to protect themselves from potential harm resulting from the breach
- Steps the covered entity is taking to investigate the breach, mitigate losses, and protect against future breaches
- Contact procedures for individuals to ask questions or receive additional information, including a toll-free telephone number, email address, website, or postal address

Covered entities must notify the Department of Health and Human Services (HHS) of all breaches. Notice to HHS must be provided immediately for breaches involving more than 500 individuals and annually for all other breaches. Covered entities have the burden of demonstrating that they satisfied the specific notice obligations following a breach, or, if notice is not made following an unauthorized use or disclosure, that the unauthorized use or disclosure did not constitute a breach. Reference Chapter 13, "Regulatory Compliance for Financial Institutions," for a further discussion of healthcare-related security incidents.

Section 13407 of the HITECH Act directed the Federal Trade Commission (FTC) to issue breach notification rules pertaining to the exposure or compromise of personal health records (PHRs). A ***personal health record*** is defined by the FTC as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." Don't confuse PHR with PHI. PHI is information that is maintained by a covered entity as defined by HIPAA/HITECH. PHR is information provided by the consumer for the consumer's own benefit. For example, if a consumer uploads and stores medical information from many sources in one online location, the aggregated data would be considered a PHR. The online service would be considered a PHR vendor.

The FTC rule applies to both vendors of PHRs (which provide online repositories that people can use to keep track of their health information) and entities that offer third-party applications for PHRs. The requirements regarding the scope, timing, and content mirror the requirements imposed on covered entities. The enforcement is the responsibility of the FTC. By law, noncompliance is considered "unfair and deceptive trade practices."

Federal Agencies

Office of Management and Budget (OMB) Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information requires all federal agencies to implement a breach notification policy to safeguard paper and digital PII. Attachment 3, "External Breach Notification," identifies the factors agencies should consider in determining when notification outside the agency should be given and the nature of the notification. Notification may not be necessary for encrypted information. Each agency is directed to establish an agency response team. Agencies must assess the likely risk of harm caused by the breach and the level of risk. Agencies should provide notification without unreasonable delay following the detection of a breach, but are permitted to delay notification for law enforcement, national security purposes, or agency needs. Attachment 3 also includes specifics as to the content of the notice, criteria for determining the method of notification, and the types of notice that may be used. Attachment 4, "Rules and Consequences Policy," states that supervisors may be subject to disciplinary action for failure to take appropriate action upon discovering the breach or failure to take the required steps to prevent a breach from occurring. Consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy.

Veterans Administration

On May 3, 2006, a data analyst at Veterans Affairs took home a laptop and an external hard drive containing unencrypted information on 26.5 million people. The computer equipment was stolen in a burglary of the analyst's home in Montgomery County, Maryland. The burglary was immediately reported to both Maryland police and his supervisors at Veterans Affairs. The theft raised fears of potential mass identity theft. On June 29, the stolen laptop computer and hard drive were turned in by an unidentified person. The incident resulted in Congress imposing specific response, reporting, and breach notification requirements on the Veterans Administration (VA).

Title IX of P.L. 109-461, the Veterans Affairs Information Security Act, requires the VA to implement agency-wide information security procedures to protect the VA's "sensitive personal information" (SPI) and VA information systems. P.L. 109-461 also requires that in the event of a "data breach" of SPI processed or maintained by the VA, the Secretary must ensure that as soon as possible after discovery, either a non-VA entity or the VA's Inspector General conduct an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any

SPI. Based on the risk analysis, if the Secretary determines that a reasonable risk exists of the potential misuse of SPI , the Secretary must provide credit protection services.

P.L. 109-461 also requires the VA to include data security requirements in all contracts with private-sector service providers that require access to SPI. All contracts involving access to SPI must include a prohibition of the disclosure of such information, unless the disclosure is lawful and expressly authorized under the contract, as well as the condition that the contractor or subcontractor notify the Secretary of any data breach of such information. In addition, each contract must provide for liquidated damages to be paid by the contractor to the Secretary in the event of a data breach with respect to any SPI, and that money should be made available exclusively for the purpose of providing credit protection services.

State Breach Notification Laws

In the absence of federal consumer breach notification law, 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted notification laws designed to protect their residents. The intent of state breach notification laws is to require companies that collect data belonging to residents of their state to notify residents of their state if there is a data breach of said information. States with no security breach law include Alabama, Kentucky, New Mexico, and South Dakota. California, Massachusetts, and Texas laws are notable:

- California was the first to adopt a security breach notification law. The California Security Breach Information Act (California Civil Code Section 1798.82), effective July 1, 2003, required companies based in California or with customers in California to notify them whenever their personal information may have been compromised. This groundbreaking legislation provided the model for states around the country.
- MA Chapter 93H Massachusetts Security Breach Notification Law, enacted in 2007, and the subsequent 201 CMR 17 Standards for the Protection of Personal Information of Residents of the Commonwealth, is widely regarded as the most comprehensive state information security legislation.
- The Texas Breach Notification Law was amended in 2011 to require entities doing business within the state to provide notification of data breaches to residents of states that have not enacted their own breach notification law. In 2013, this provision was removed. Additionally, in 2013, an amendment was added that notice provided to consumers in states that require notification can comply with either the Texas law or the law of the state in which the individual resides.

The basic premise of the state security breach laws is that consumers have a right to know if unencrypted personal information such as SSN, driver's license number, state identification card number, credit or debit card number, account password, PINs, or access codes have either been or are suspected to be compromised. The concern is that the listed information could be used fraudulently to assume or attempt to assume a person's identity. Exempt from legislation is publicly available information that is lawfully made available to the general public from federal, state, or local government records or by widely distributed media.

State security breach notification laws generally follow the same framework, which includes who must comply, a definition of personal information and breach, the elements of harm that must occur, triggers for notification, exceptions, and the relationship to federal law and penalties and enforcement authorities. Although the framework is standard, the laws are anything but. The divergence begins with the differences in how personal information is defined and who is covered by the law, and ends in aggregate penalties that range from $50,000 to $500,000. The variations are so numerous that compliance is confusing and onerous.

It is strongly recommended that any organization that experiences a breach or suspected breach of PII consult with legal counsel for interpretation and application of the myriad of sector-based, federal, and state incident response and notification laws.

FYI: State Security Breach Notification Laws

As of October 2013, 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.

The National Conference of State Legislatures maintains a public access library of state security breach notification laws and related legislation at www.ncsl.org/research/telecommunications-and-information-technology/overview-security-breaches.aspx.

Does Notification Work?

In the previous section, we discussed sector-based, federal, and state breach notification requirements. Notification can be resource intensive, time consuming, and expensive. The question that needs to be asked is, is it worth it? The resounding answer from privacy and security advocates, public relations (PR) specialists, and consumers is "yes." Consumers trust those who collect their personal information to protect it. When that doesn't happen, they need to know so that they can take steps to protect themselves from identity theft, fraud, and privacy violations.

In June 2012, Experian commissioned the Ponemon Institute to conduct a consumer study on data breach notification. The findings are instructive. When asked "What personal data if lost or stolen would you worry most about?", they overwhelmingly responded "password/PIN" and "Social Security number."

- Eighty-five percent believe notification about data breach and the loss or theft of their personal information is relevant to them.
- Fifty-nine percent believe a data breach notification means there is a high probability they will become an identity theft victim.

- Fifty-eight percent say the organization has an obligation to provide identity protection services, and 55% say they should provide credit-monitoring services.
- Seventy-two percent were disappointed in the way the notification was handled. A key reason for the disappointment is respondents' belief that the notification did not increase their understanding about the data breach.

FYI: Security Breach Notification Website

New Hampshire law requires organizations to notify the Office of the Attorney General of any breach that impacts New Hampshire residents. Copies of all notifications are posted on the NH Department of Justice, Office of the Attorney General website at http://doj.nh.gov/consumer/security-breaches/.

In Practice

Data Breach Reporting and Notification Policy

Synopsis: To ensure compliance with all applicable laws, regulations, and contractual obligations, timely communications with customers, and internal support for the process.

Policy Statement:

- It is the intent of the company to comply with all information security breach–related laws, regulations, and contractual obligations.
- Executive management has the authority to engage outside expertise for legal counsel, crisis management, PR, and communications.
- Affected customer and business partners will be notified as quickly as possible of a suspected or known compromise of personal information. The company will provide regular updates as more information becomes known.
- Based on applicable laws, legal counsel in collaboration with the CEO will make the determination regarding the scope and content of customer notification.
- Legal counsel and the marketing/PR department will collaborate on all internal and external notifications and communications. All publications must be authorized by executive management.
- Customer service must staff appropriately to meet the anticipated demand for additional information.
- The COO is the official spokesperson for the organization. In his/her absence, the legal counsel will function as the official spokesperson.

The Public Face of a Breach

It's tempting to keep a data breach secret, but not reasonable. Consumers need to know when their information is at risk so they can respond accordingly. Once notification has gone out, rest assured that the media will pick up the story. Breaches attract more attention than other technology-related topic, so reporters are more apt to cover them to drive traffic to their sites. If news organizations learn about these attacks through third-party sources while the breached organization remains silent, the fallout can be significant. Organizations must be proactive in their PR approach, using public messaging to counteract inaccuracies and tell the story from their point of view. Doing this right can save an organization's reputation and even, in some cases, enhance the perception of its brand in the eyes of customers and the general public. The PR professionals advise following these straightforward but strict rules when addressing the media and the public:

- Get it over with.
- Be humble.
- Don't lie.
- Say only what needs to be said.

Don't wait until a breach happens to develop a RP preparedness plan—communications should be part of any incident preparedness strategy. Security specialists should work with PR people to identify the worst possible breach scenario so they can message against it and determine audience targets, including customers, partners, employees, and the media. Following a breach, messaging should be bulletproof and consistent.

FYI: Small Business Note

Most small businesses don't see themselves as a target. However, according to the 2013 Verizon Data Breach Incident Report, 75% of attacks are opportunistic—not targeted at a specific individual or company.

Of the incidents investigated by Verizon:

- Seventy-eight percent of intrusions took little or no specialist skills or resources.
- Seventy-six percent of intrusions exploited weak or stolen credentials.
- Forty percent of intrusions involved malware.
- Twenty-nine percent of intrusions used social tactics to gain information.

Training users to use strong passwords, not click on email embedded links, not open unsolicited email attachments, properly identify anyone requesting information, and report suspicious activity can significantly reduce small business exposure and harm.

Summary

An information security incident is an adverse event that threatens business security and/or disrupts operations. Examples include intentional unauthorized access, DDoS attacks, malware, and inappropriate usage. The objective of an information security risk management program is to minimize the number of successful attempts and attacks. The reality is that security incidents happen even at the most security-conscious organizations. Every organization should be prepared to respond to an incident quickly, confidently, and in compliance with applicable laws and regulations.

The objective of incident management is a consistent and effective approach to the identification of and response to information security–related incidents. Meeting that objective requires situational awareness, incident reporting mechanisms, a documented IRP, and an understanding of legal obligations. Incident preparation includes developing strategies and instructions for documentation and evidence handling, detection and investigation (including forensic analysis), containment, eradication and recovery, notification, and closure. The roles and responsibilities of key personnel, including executive management, legal counsel, incident response coordinators (IRCs), designated incident handlers (DIHs), the incident response team (IRT), and ancillary personnel as well as external entities such as law enforcement and regulatory agencies, should be clearly defined and communicated. Incident response capabilities should be practiced and evaluated on an ongoing basis.

Consumers have a right to know if their personal data has been compromised. In most situations, data breaches of PII must be reported to the appropriate authority and affected parties notified. A data breach is generally defined as actual or suspected compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or unauthorized use or loss of control of legally protected PII. Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted consumer notification laws designed to protect their residents. In addition to state laws, there are sector- and agency-specific federal regulations that pertain to reporting and notification. Organizations that experience a breach or suspected breach of PII should consult with legal counsel for interpretation and application of often overlapping and contradictory rules and expectations.

Incident management policies include Incident Definition Policy, Incident Classification Policy, Information Response Program Policy, Incident Response Authority Policy, Evidence Handling and Use Policy, and Data Breach Reporting and Notification Policy.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following statements best defines incident management?

   A. Incident management is risk minimization.

   B. Incident management is a consistent approach to responding to and resolving issues.

   C. Incident management is problem resolution.

   D. Incident management is forensic containment.

2. Which of the following statements is true of security-related incidents?

   A. Over time, security-related incidents have become less prevalent and less damaging.

   B. Over time, security-related incidents have become more prevalent and more disruptive.

   C. Over time, security-related incidents have become less prevalent and more damaging.

   D. Over time, security-related incidents have become more numerous and less disruptive.

3. Minimizing the number of incidents is a function of which of the following?

   A. Incident response testing

   B. Forensic analysis

   C. Risk management

   D. Security investments

4. An information security incident can ___________.

   A. compromise business security

   B. disrupt operations

   C. impact customer trust

   D. All of the above

5. Which of the following statements is true when an information security–related incident occurs at a business partner or vendor who hosts or processes legally protected data on behalf of an organization?

   A. The organization does not need to do anything.

   B. The organization must be notified and respond accordingly.

   C. The organization is not responsible.

   D. The organization must report the incident to local law enforcement.

6. Which of the following attack types best describes a targeted attack that successfully obstructs functionality?

   A. Spam attack

   B. Malware attack

   C. DDoS attack

   D. Killer attack

7. A celebrity is admitted to the hospital. If an employee accesses the celebrity's patient record just out of curiosity, the action is referred to as __________.

   A. inappropriate usage

   B. unauthorized access

   C. unacceptable behavior

   D. undue care

8. Employees who report incidents should be ___________.

   A. prepared to assign a severity level

   B. praised for their actions

   C. provided compensation

   D. None of the above

9. Which of the following statements is true of an incident response plan?

   A. An incident response plan should be updated and authorized annually.

   B. An incident response plan should be documented.

   C. An incident response plan should be stress tested.

   D. All of the above

10. Which of the following terms best describes a signal or warning that an incident may occur in the future?

    A. A sign

    B. A precursor

    C. An indicator

    D. Forensic evidence

11. Which of the following terms best describes the process of taking steps to prevent the incident from spreading?

    A. Detection
    B. Containment
    C. Eradication
    D. Recovery

12. Which of the following terms best describes the addressing of the vulnerabilities related to the exploit or compromise and restoring normal operations?

    A. Detection
    B. Containment
    C. Testing
    D. Recovery

13. Which of the following terms best describes the eliminating of the components of the incident?

    A. Investigation
    B. Containment
    C. Eradication
    D. Recovery

14. Which of the following terms best describes the substantive or corroborating evidence that an incident may have occurred or may be occurring now?

    A. Indicator of compromise
    B. Forensic proof
    C. Heresy
    D. Diligence

15. Which of the following is not generally an incident response team responsibility?

    A. Incident impact analysis
    B. Incident communications
    C. Incident plan auditing
    D. Incident management

16. Incident response activity logs should *not* include which of the following?

A. Date
B. Time
C. Decisions made
D. Cost of the activity

17. The decision to contact law enforcement should be made ______________.

A. early in the incident lifecycle
B. once an incident has been verified
C. after evidence has been collected
D. only if there is a loss of funds

18. Which of the following agencies' investigative responsibilities include financial fraud, money laundering, and identity theft?

A. FBI
B. Department of Homeland Security
C. Secret Service
D. State Police

19. Documentation of the transfer of evidence is known as a ____________.

A. chain of evidence
B. chain of custody
C. chain of command
D. chain of investigation

20. Data breach notification laws pertain to which of the following?

A. Intellectual property
B. Patents
C. PII
D. Products

21. Federal breach notification laws apply to _____________.

A. specific sectors such as financial and healthcare
B. all United States citizens
C. any disclosure of a Social Security number
D. None of the above

22. HIPAA/HITECH requires ______________ within 60 days of the discovery of a breach.

    A. notification be sent to affected parties

    B. notification be sent to law enforcement

    C. notification be sent to Department of Health and Human Services

    D. notification be sent to all employees

23. With the exception of the ___________, all federal agencies are required to act in accordance with OMB M-07-16: "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" guidance.

    A. Department of Health and Human Services

    B. Federal Reserve

    C. Internal Revenue Service

    D. Veterans Administration

24. Which of the following statements is true of state breach notification laws?

    A. Notification requirements are the same in every state.

    B. State laws exist because there is no comparable federal law.

    C. Every state has a state breach notification law.

    D. The laws only apply to verified breaches.

25. Which of the following states was the first state to enact a security breach notification law?

    A. Massachusetts

    B. Puerto Rico

    C. California

    D. Alabama

26. Which of the following statements is true concerning the Texas security breach notification law?

    A. The Texas security breach notification law includes requirements that in-state businesses provide notice to residents of all states.

    B. The Texas security breach notification law includes requirements that in-state businesses only provide notice to residents of Texas.

    C. The Texas security breach notification law includes requirements that in-state businesses are exempt from notification requirements.

    D. The Texas security breach notification law includes requirements that in-state businesses provide notice internationally.

27. Consumers are most concerned about compromise of their _______________.

- **A.** password/PIN and SSN
- **B.** email address
- **C.** checking account number
- **D.** address and date of birth

28. Which of the following statements is true?

- **A.** Consumers want to be notified of a data breach and they overwhelmingly expect to be compensated.
- **B.** Consumers want to be notified of a data breach and they overwhelmingly expect to be provided as much detail as possible.
- **C.** Consumers want to be notified of a data breach and they overwhelmingly expect to be told when the criminal is apprehended.
- **D.** Consumers want to be notified of a data breach and they overwhelmingly expect to be interviewed by investigators.

29. Incident response plans and procedures should be tested ____________.

- **A.** during development
- **B.** upon publication
- **C.** on an ongoing basis
- **D.** only when there are changes

30. The Board of Directors (or equivalent body) is responsible for ____________.

- **A.** the cost of notification
- **B.** contacting regulators
- **C.** managing response efforts
- **D.** authorizing incident response policies

EXERCISES

EXERCISE 11.1: Assessing an Incident Report

1. At your school or workplace, locate information security incident reporting guidelines.
2. Evaluate the process. Is it easy to report an incident? Are you encouraged to do so?
3. How would you improve the process?

EXERCISE 11.2: Evaluating an Incident Response Policy

1. Locate an incident response policy document either at your school, workplace, or online. Does the policy clearly define the criteria for an incident?
2. Does the policy define roles and responsibilities? If so, describe the response structure (for example, who is in charge, who should investigate an incident, who can talk to the media). If not, what information is the policy missing?
3. Does the policy include notification requirements? If yes, what laws are referenced and why? If no, what laws should be referenced?

EXERCISE 11.3: Researching Containment and Eradication

1. Research and identify the latest strains of malware.
2. Choose one. Find instructions for containment and eradication.
3. Conventional risk management wisdom is that it is better to replace a hard drive than to try to remove malware. Do you agree? Why or why not?

EXERCISE 11.4: Researching a DDoS Attack

1. Find a recent news article about DDoS attacks.
2. Who were the attackers and what was their motivation?
3. What was the impact of the attack? What should the victim organization do to mitigate future damage?

EXERCISE 11.5: Understanding Evidence Handling

1. Create a worksheet that could be used by an investigator to build an "incident profile."
2. Create an evidentiary "chain of custody" form that could be used in legal proceedings.
3. Create a log for documenting forensic or computer-based investigation.

PROJECTS

PROJECT 11.1: Creating Incident Awareness

1. One of the key messages to be delivered in training and awareness programs is the importance of incident reporting. Educating users to recognize and report suspicious behavior is a powerful deterrent to would-be intruders. The organization you work for has classified the following events as high priority, requiring immediate reporting:
   - Customer data at risk of exposure or compromise
   - Unauthorized use of a system for any purpose

- DoS attack
- Unauthorized downloads of software, music, or videos
- Missing equipment
- Suspicious person in the facility

You have been tasked with training all users to recognize these types of incidents.

1. Write a brief explanation of why each of the listed events is considered high priority. Include at least one example per event.
2. Create a presentation that can be used to train employees to recognize these incidents and how to report them.
3. Create a ten-question quiz that tests their post-presentation knowledge.

PROJECT 11.2: Assessing Security Breach Notifications

Access the State of New Hampshire, Department of Justice, Office of the Attorney General security breach notification web page. Sort the notifications by year.

1. Read three recent notification letters to the Attorney General as well as the corresponding notice that will be sent to the consumer (be sure to scroll through the document). Write a summary and timeline (as presented) of each event.
2. Choose one incident to research. Find corresponding news articles, press releases, and so on.
3. Compare the customer notification summary and timeline to your research. In your opinion, was the notification adequate? Did it include all pertinent details? What controls should the company put in place to prevent this from a happening again?

PROJECT 11.3: Comparing and Contrasting Regulatory Requirements

The objective of this project is to compare and contrast breach notification requirements.

1. Create a grid that includes state, statute, definition of personal information, definition of a breach, timeframe to report a breach, reporting agency, notification requirements, exemptions, and penalties for nonconformance. Fill in the grid using information from five states.
2. If a company who did business in all five states experienced a data breach, would it be able to use the same notification letter for consumers in all five states? Why or why not?
3. Create a single notification law using what you feel are the best elements of the five laws included in the grid. Be prepared to defend your choices.

Case Study

An Exercise in Cybercrime Incident Response

A cybercrime incident response exercise is one of the most effective ways to enhance organizational awareness. This cybercrime incident response exercise is designed to mimic a multiday event. Participants are challenged to find the clues, figure out what to do, and work as a team to minimize the impact. Keep the following points in mind:

- Although fictional, the scenarios used in the exercise are based on actual events.
- As in the actual events, there may be "unknowns" and it may be necessary to make some assumptions.
- The scenario will be presented in a series of situation vignettes.
- At the end of each day, you will be asked to answer a set of questions. Complete the questions before continuing on.
- At the end of Day 2, you will be asked to create a report.

This Case Study is designed to be a team project. You will need to work with at least one other member of your class to complete the exercise.

Background

BestBank is proudly celebrating its tenth anniversary year with special events throughout the year. Last year, BestBank embarked on a five-year strategic plan to extend its reach and offer services to municipalities and armed services personnel. Integral to this plan is the acquisition of U.S. Military Bank. The combined entity will be known as USBEST. The new entity will be primarily staffed by BestBank personnel.

USBEST is maintaining U.S. Military Bank's long-term contract with the Department of Defense to provide financial and insurance services to active-duty and retired military personnel. The primary delivery channel is via a branded website. Active-duty and retired military personnel can access the site directly by going to www.bankformilitary.org. USBEST has also put a link on its home page. The bankformilitary.org website is hosted by HostSecure, a private company located in the Midwest.

USBEST's first marketing campaign is a "We're Grateful" promotion, including special military-only certificate of deposit (CD) rates as well as discounted insurance programs.

Cast of Characters:

- Sam Smith, VP of Marketing
- Robyn White, Deposit Operations and Online Banking Manager
- Sue Jones, IT Manager
- Cindy Hall, Deposit Operations Clerk
- Joe Bench, COO

Day 1

Wednesday 7:00 A.M.

The marketing campaign begins with posts on Facebook and Twitter as well as emails to all current members of both institutions announcing the acquisition and the “We’re Grateful” promotion. All communications encourage active-duty and retired military personnel to visit the www.bankformilitary.org website.

Wednesday 10:00 A.M.

IT sends an email to Sam Smith, VP of Marketing, reporting that they have been receiving alerts that indicate there is significant web traffic to http://www.bankformilitary.org. Smith is pleased.

Wednesday Late Morning/Early Afternoon

By late morning, the USBEST receptionist starts getting calls about problems accessing the bankformilitary.org site. After lunch, the calls escalate; the callers are angry about something on the website. As per procedure, she informs callers that the appropriate person will call them back as soon as possible and forwards the messages to Sam Smith’s voicemail.

Wednesday 3:45 P.M.

Sam Smith returns to his office and retrieves his voice messages. Smith opens his browser and goes to bankformilitary.org. To his horror, he finds that “We’re Grateful” has been changed to “We’re Hateful” and that “USBEST will be charging military families fees for all services.”

Sam immediately goes to the office of Robyn White, Deposit Operations and Online Banking Manager. Robyn’s department is responsible for online services, including the bankformilitary.org website, and she has administrative access. He is told that Robyn is working remotely and that she has email access. Sam calls Robyn at home but gets her voicemail. He sends her an email asking her to call him ASAP!

Sam then contacts the bank’s IT Manager, Sue Jones. Sue calls HostSecure for help in gaining access to the website. HostSecure is of little assistance. They claim that all they do is host, not manage the site. Sue insists upon talking to “someone in charge.” After being transferred and put on hold numerous times, she speaks with the HostSecure Security Officer, who informs her that upon proper authorization, they can shut down the website. Jones inquires who is on the authorization list. The HostSecure Security Officer informs Sue that it would be a breach of security to provide that information.

Wednesday 4:40 P.M.

Sue Jones locates Robyn White’s cell phone number and calls her to discuss what is happening. Robyn apologizes for not responding quicker to Sam’s mail; she ducked out for her son’s soccer game. Robyn tells Sue that she had received an email early this morning from HostSecure informing her that she needed to update her administrative password to a more secure version. The email had a link to a change password form. She was happy to learn that they were updating their password requirements. Robyn reported that she clicked the link, followed the instructions (which included verifying her current password), and changed her password to a secure, familiar one. She also forwarded the email to Cindy Hall, Deposit Operations Clerk, and asked her to update her password as well. Sue asks Robyn to log in to bankformilitary.org to edit the home page. Robyn complies and logs in with her new credentials. The login screen returns a "bad password" error. She logs in with her old credentials; they do not work either.

Wednesday 4:55 P.M.

Sue Jones calls HostSecure. She is put on hold. After waiting five minutes, she hangs up and calls again. This time she receives a message that regular business hours are 8:00 a.m. to 5:00 p.m. EST. The message indicates that for emergency service, customers should call the number on their service contract. Sue does not have a copy of the contract. She calls the Accounting and Finance Department Manager to see if they have a copy. Everyone in the department is gone for the day.

Wednesday 5:10 P.M.

Sue Jones lets Sam Smith know that she cannot do anything more until the morning. Sam decides to update Facebook and the USBEST website home page with an announcement of what is happening, reassuring the public that the bank is doing everything they can and apologizing profusely.

Day 1 Questions:

1. What do you suspect is happening or has happened?
2. What actions (if any) should be taken?
3. Who should be contacted and what should they be told?
4. What lessons can be learned from the day's events?

Day 2

Thursday 7:30 A.M.

Cindy Hall's first task of the day is to log in to the bankformilitary.org administrative portal to retrieve a report on the previous evening's transactional activity. She is surprised to see so many Bill Pay transactions. Upon closer inspection, the funds all seem to be going to the same account and they started a few minutes after midnight. She makes an assumption that the retailer must be having a midnight special and wonders what it is. She then opens Outlook and sees Robyn's forwarded email about changing her password. She proceeds to do so.

Thursday 8:00 A.M.

Customer Service opens at 8:00 a.m. Immediately they begin fielding calls from military personnel reporting fraudulent Bill Pay transactions. The CSR manager calls Cindy Hall in Deposit Operations to report the problem. Cindy accesses the bankformilitary.org administrative portal to get more information but finds she cannot log in. She figures she must have written down her new password incorrectly. She will ask Robyn to reset it when she gets in.

Thursday 8:30 A.M.

Robyn arrives for work and plugs in her laptop.

Thursday 9:00 A.M.

Sam Smith finally gets through to someone at HostSecure who agrees to work with him to remove the offending text. He is very relieved and informs Joe Bench, COO.

Thursday 10:10 A.M.

Sam Smith arrives ten minutes late to the weekly senior management meeting. He is visibly shaken. He connects his iPad to a video projector and displays on the screen an anonymous blog that is describing the defacement, lists the URL for the bankformilitary.org administrative portal, the username and password for an administrative account, and member account information. He scrolls down to the next blog entry, which includes private internal bank correspondence.

Day 2 Questions:

1. What do you suspect is happening or has happened?
2. Who (if anyone) external to the organization should be notified?
3. What actions should be taken to contain the incident and minimize the impact?
4. What should be done post-containment?
5. What lessons can be learned from the day's events?

Day 2 Report

It is now 11:00 a.m. An emergency meeting of the Board of Directors has been called for 3:30 p.m. You are tasked with preparing a written report for the Board that includes a synopsis of the incident, detailing the response effort up to the time of the meeting, and recommending a timeline of next steps.

Day 2: Presentation to the Board of Directors 3:30 P.M.

1. Present your written report to the Board of Directors.
2. Be prepared to discuss next steps.
3. Be prepared to discuss law enforcement involvement (if applicable).
4. Be prepared to discuss consumer notification obligations (if applicable).

References

Regulations Cited

"16 C.F.R. Part 318: Health Breach Notification Rule: Final Rule—Issued Pursuant to the American Recovery and Reinvestment Act of 2009—Requiring Vendors of Personal Health Records and Related Entities To Notify Consumers When the Security of Their Individually Identifiable Health Information Has Been Breached," Federal Trade Commission, accessed 10/2013, www2.ftc.gov/opa/2009/08/hbn.shtm.

"Appendix B to Part 364—Interagency Guidelines Establishing Information Security Standards," accessed 08/2013, www.fdic.gov/regulations/laws/rules/2000-8660.html.

"201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth," official website of the Office of Consumer Affairs & Business Regulation (OCABR), accessed 05/06/2013, www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

"Family Educational Rights and Privacy Act (FERPA)," official website of the U.S. Department of Education, accessed 05/2013, www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

"Financial Institution Letter (FIL-27-2005), Final Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," accessed 10/2013, www.fdic.gov/news/news/financial/2005/fil2705.html.

"HIPAA Security Rule," official website of the Department of Health and Human Services, accessed 05/2013, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

"Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules 45 CFR Parts 160 and 164 Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule," *Federal Register*, Volume 78, No. 17, January 25, 2013, accessed 06/2013, www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/.

"Office of Management and Budget Memorandum M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information," accessed 10/2013, www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.

State of California, "SB 1386: California Security Breach Information Act, Civil Code Section 1798.80-1798.84," Official California Legislative Information, accessed 05/2013, www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84.

State of Texas, Business and Commerce Code, Sections 521.053, accessed 10/2013, ftp://ftp.legis.state.tx.us/bills/83R/billtext/html/senate_bills/SB01600_SB01699/SB01610H.htm.

Other References

"2012 Consumer Study on Data Breach Notification," Ponemon Institute, LLC, June 2012, accessed 10/2013, www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf.

"Chain of Custody and Evidentiary Issues," eLaw Exchange, accessed 10/2013, www.elawexchange.com.

"Complying with the FTC's Health Breach Notification Rule," April 2010, FTC Bureau of Consumer Protection, accessed 10/2013, www.business.ftc.gov/documents/bus56-complying-ftcs-health-breach-notification-rule.

"Consumer Study on Data Breach Notification" Ponemon Institute, LLC, 2012, accessed 10/2013, www.experian.com/data-breach/ponemon-notification-study.html.

"Data Breach Response Checklist PTAC-CL, September 2012," Department of Education, Privacy Technical Assistance Center, accessed 10/2013, http://ptac.ed.gov/document/checklist-data-breach-response-sept-2012.

"Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition," U.S. Department of Justice, National Institute of Justice, April 2008, accessed 10/2013, www.nij.gov/nij/pubs-sum/219941.htm.

"Forensic Examination of Digital Evidence: A Guide for Law Enforcement," U.S. Department of Justice, National Institute of Justice, April 2004, accessed 10/2013, www.nij.gov/pubs-sum/199408.htm.

"FTC Issues Final Breach Notification Rule for Electronic Health Information," Federal Trade Commission, accessed 10/2013, www2.ftc.gov/opa/2009/08/hbn.shtm.

"Incident Response Procedures for Data Breaches, 0900.00.01," U.S. Department of Justice, August 6, 2013, accessed October 2013, www.justice.gov/opcl/breach-procedures.pdf.

"Information Technology Security Incident Response Plan v1.0," February 15, 2010, University of Connecticut, accessed 10/2013, http://security.uconn.edu/wp-content/blogs.dir/14/files/2010/07/security-incident-response-procedures.pdf.

"IT Security Incident Response HIPAA Policy 01/02/2012," Yale University, accessed 10/2013, www.yale.edu/ppdev/policy/5143/5143.pdf.

"Largest Incidents," DataLossdb Open Security Foundation, accessed 10/2013, www.datalossdb.org.

Lee, Christopher and Zachary A. Goldfarb. "Stolen VA Laptop and Hard Drive Recovered," *Washington Post*, Friday, June 30, 2006, accessed 2013, www.washingtonpost.com/wp-dyn/content/article/2006/06/29/AR2006062900352.html.

Mandia, Kevin and Chris Prosise. Incident Response: Investigating Computer Crime, Berkeley, California: Osborne/McGraw-Hill, 2001.

Nolan, Richard, “First Responders Guide to Computer Forensics,” 2005, Carnegie Mellon University Software Engineering Institute.

“Pennsylvania Man Pleads Guilty to Hacking into Multiple Computer Networks,” U.S. Attorney’s Office, August 27, 2013, District of Massachusetts, Federal Bureau of Investigation, accessed 10/2013, www.fbi.gov/boston/press-releases/2013/pennsylvania-man-pleads-guilty-to-hacking-into-multiple-computer-networks.

Proffit, Tim, “Creating and Maintaining Policies for Working with Law Enforcement,” 2008, SANS Institute.

“Responding to IT Security Incidents,” Microsoft Security TechCenter, accessed 10/2013, http://technet.microsoft.com/en-us/library/cc700825.aspx.

“Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,” United States Department of Justice, accessed 10/2013, www.cybercrime.gov/s&smanual2002.htm.

“Security Breach Notification Legislation/Laws,” National Conference of State Legislatures, accessed 10/2013, www.ncsl.org/research/telecommunications-and-information-technology/overview-security-breaches.aspx.

Stevens, Gina, “Data Security Breach Notification Laws,” April 20, 2012, Congressional Research Service, accessed 10/2013, www.crs.gov.

“Texas amends data breach notification law to remove out-of-state obligations,” Winston and Strawn, LLP, accessed 10/2013, www.lexology.com/library/detail.aspx?g=eda7fb1a-a4a4-4041-8966-e65137c9d5e9.

“The Massachusetts Data Security Law and Regulations,” McDermott, Will & Emery, November 2, 2009, accessed 10/2013, www.mwe.com.

“United States Computer Emergency Readiness Team,” US-CERT, accessed 10/2013, www.us-cert.gov/.

“2013 Data Breach Investigations Report, Verizon,” Verizon, accessed 10/2013, www.verizonenterprise.com/DBIR/2013.

Chapter 12

Business Continuity Management

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Define a disaster.
- Appreciate the importance of emergency preparedness.
- Analyze threats, risks, and business impact assessments.
- Explain the components of a business continuity plan and program.
- Develop policies related to business continuity management.

Section 14 of the ISO 27002:2013 is “Business Continuity Management.” The objective of the Business Continuity Management domain is to ensure the continued operation and secure provision of essential services during a disruption of normal operating conditions. To support this objective, threat scenarios are evaluated, essential services and processes are identified, and response, contingency, and recovery and resumption strategies, plans, and procedures are developed, tested, and maintained. Business continuity is a component of organization risk management.

We have learned valuable lessons from the events of September 11, 2001, Hurricane Katrina, and the 2013 Boston bombing. Preparation and business continuity plans do more than protect business assets; in the long run, they protect employees and their families, investors, business partners, and the community. Business continuity plans are, in essence, a civic duty.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 14 of the ISO 27002:2013, "Business Continuity Management," focuses on availability and the secure provision of essential services during a disruption of normal operating conditions. ISO 22301 provides a framework to plan, establish, implement, operate, monitor, review, maintain, and continually improve a business continuity management system (BCMS).

Corresponding NIST guidance is provided in the following documents:

- SP 800-34: Contingency Planning Guide for Information Technology System, Revision 1
- SP 800-84: Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities

Emergency Preparedness

A ***disaster*** is an event that results in damage or destruction, loss of life, or drastic change to the environment. In a business context, a disaster is an unplanned event that has the potential to disrupt the delivery of mission-critical services and functions, jeopardize the welfare of employees, customers, or business partners, and/or cause significant financial harm. From a security perspective, a disaster manifests itself as a sustained disruption of system availability and/or confidentiality or integrity controls. The cause can be environmental, operational, accidental, or willful:

- ***Environmental events*** include severe weather, earthquakes, tornados, fire, flood, air contaminants, and public health emergencies.
- ***Operational issues*** include failures or misconfiguration of equipment, disruption of communication systems, unavailability of third-party systems or personnel, and degradation of power.
- ***Accidents*** include nuclear, biological, or hazardous chemical exposure, explosions, and user or operator error.
- ***Willful damage*** includes terrorism, sabotage, civil disturbances, war, workplace violence, and cybercrime.

Worldwide, a major disaster occurs almost daily. According to the Federal Emergency Management Agency (FEMA), a disaster has occurred, on average, every week in the United States for the past ten years. The U.S. Department of Homeland Security (DHS) has identified the impact of 15 disaster scenarios that could take the country days (explosives) to weeks (food contamination) to months (pandemic, major hurricane) to years (nuclear detonation, major earthquake) to potentially recover from.

Preparing for a disaster can make the difference between life and death, success or failure, yet most businesses are not prepared. An Ad Council survey found that nearly two-thirds (62%) of respondents did not have an emergency plan in place for their business. When disaster inevitably strikes, without a plan, there is little chance of a successful response and recovery. The Insurance Information Institute reported that up to 40% of businesses affected by a natural or human-caused disaster never reopen.

The goal of emergency preparedness is to protect life and property. Disasters are unplanned; however, they should not be unanticipated. How much an organization should prepare depends on a number of factors, including risk tolerance, financial strength, regulatory requirements, and stakeholder impact. What we know for sure is that relying solely on insurance and post-disaster government assistance is shortsighted and, in some cases, negligent.

What Is a Resilient Organization?

A ***resilient*** organization is one that has the ability to quickly adapt and recover from known or unknown changes to the environment. Resilience doesn't just happen. It requires management support, investment, planning, and layers of preparation. In their post-9/11 study, "The Five Principles of Organizational Resilience," Gartner reminds us that "organizational resilience has taken on a new urgency since the tragic events of Sept. 11. The ability to respond quickly, decisively and effectively to unforeseen and unpredictable forces is now an enterprise imperative." It cites leadership, culture, people, systems, and settings as the bedrock of an agile and adaptive organization.

- Resilience begins with enterprise leadership setting the priorities, allocating the resources, and making the commitments to establish organizational resilience throughout the enterprise.
- A resilient culture is built on principles of organizational empowerment, purpose, trust, and accountability.
- People who are properly selected, motivated, equipped, and led will overcome almost any obstacle or disruption.
- Organizations achieve agility and flexibility by combining a highly distributed workplace model with a highly robust and collaborative IT infrastructure.
- Alternative workplace techniques such as office "hoteling," telecommuting, and desk sharing provide the level of workplace flexibility and agility that is essential for mitigating the risk of catastrophic or disruptive incidents.

Regulatory Requirements

Business disruption has an economic and societal ripple effect. Emergency preparedness is a civic duty and, in many cases, a regulatory requirement. In 1998, President Clinton issued *Presidential Decision Directive (PDD) 63 Critical Infrastructure Protection*. The first in a series of executive branch directives, PDD-63 outlined roles, responsibilities, and objectives for protecting the nation's utility, transportation, financial, and other essential infrastructure, and introduced the concept of public-private partnership. In 2003, President Bush, issued *Presidential Directive HSPD-7 Critical Infrastructure Identification, Prioritization, and Protection* (Bush), which designates certain sectors of the national infrastructure as critical to the national and economic security of the United States and the well-being of its citizenry, and requires steps be taken to protect it, including emergency response and continuity measures.

Congress recognized the issue as well and included emergency preparedness in critical sector regulatory legislation. The Health Insurance Portability and Accountability Act (HIPAA) Contingency Plan Standard 164.308(a)(7) requires covered entities to “Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.” The standard includes implementation specifications for data backup, disaster recovery, and emergency mode operation plans. The Gramm-Leach-Bliley Safeguards Act requires financial institutions to “identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems” and to “take measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.” Similar legislation has been issued by the Federal Energy Regulatory Commission (FERC) for utility companies, by the Nuclear Energy Regulatory Commission (NERC) for nuclear power plants, by the Federal Communications Commission (FCC) for telecom carriers, and by the Food and Drug Administration (FDA) for pharmaceutical companies.

In October 2012, the Department of Homeland Security issued *Federal Continuity Directive 1*. The directive states that “Federal Executive Branch organizations, regardless of their size or location, shall have in place a viable continuity capability to ensure resiliency and continued performance of their organization’s essential functions under all condition.” Included in the directive was a restatement of the government’s roles in creating public/private partnerships in order to create and sustain a “culture of continuity.”

In May 2012, NIST released Special Publication 800-34, R1: Contingency Planning Guide for Federal Information Systems, which provides guidance for federal agencies. The guidance is applicable to public and private sector business continuity planning.

FYI: Devastated by an F4 Tornado

The individuals who work at Aeneas Internet and Telephone of Jackson, Tennessee, know what it’s like to have their business devastated by Mother Nature. Fortunately, because they had a disaster recovery plan, they also know what it’s like to recover from devastation. On May 4, 2003, Aeneas was among the more than 400 businesses in Tennessee hit by an F4 tornado, packing winds greater than 200 miles per hour. The tornado resulted in 11 deaths and more than $50 million in damage throughout the community. Aeneas Internet and Telephone lost more than $1 million in hardware and software, and its home office was reduced to rubble.

"There was nothing left of our building. Just piles of bricks and concrete. We lost everything," said Aeneas Internet and Telephone CEO Jonathan Harlan. "But backup systems were in place and our employees worked from other locations. And because we were ready, our customers never knew the difference." Less than 72 hours later Aeneas was back, fully serving its clients' needs. In fact, many of its smaller business and residential phone customers never lost their service. Aeneas had been able to protect itself against a worst-case scenario because it had planned for a worst-case scenario. Its business recovery plan was based on the idea that even if its facilities were destroyed and services halted, it would have backups in place and ready to go. Through the recovery effort, Aeneas officials were careful to keep customers abreast of their progress. Aeneas also benefited from the quick work and dynamic spirit of its employees and the local community who refused to let a tornado bring down what they had fought so hard to build in the first place.

In Practice

Emergency Preparedness Policy

Policy Synopsis: Demonstrate the organization's commitment to emergency preparedness and business continuity.

Policy Statement:

- An emergency preparedness and business continuity strategy that ensures the safety of employees and customers, enables the company to perform essential functions absent normal operating conditions, protects organizational assets, and meets regulatory requirements is an organizational priority.
- The company will designate necessary resources to develop and maintain emergency preparedness and business continuity plans and procedures.

Business Continuity Risk Management

Continuity planning is simply the good business practice of ensuring the execution of essential functions. Continuity planning is an integral component of organizational risk management. In Chapter 4, "Governance and Risk Management," we defined risk management as the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken. Risk management for continuity of operations requires that organizations identify threats (threat assessment), determine risk (risk assessment), and assess the internal and external impact of the disruption of mission-critical or essential services (business impact assessment). The two anticipated outcomes are (1) the identification and (if feasible) mitigation of significant threats and (2) the documentation of essential services. This information is then used to construct response, continuity, and recovery operations.

What Is a Business Continuity Threat Assessment?

A ***business continuity threat*** can best be defined as a potential danger to the organization. Threats can be business specific, local, regional, national, or even global. The objective of a ***business continuity threat assessment*** is to identify viable threats and predict the likelihood of occurrence. Threat modeling takes into account historical and predictive geographic, technological, physical, environmental, third-party, and industry factors such as the following:

- What type of disasters have occurred in the community or at this location?
- What can happen due to the geographic location?
- What could cause processes or information systems to fail?
- What threats are related to service provider dependency?
- What disasters could result from the design or construction of the facility or campus?
- What hazards are particular to the industry sector?

Identified threats are rated in terms of the likelihood of occurrence and potential impact sans controls. The higher the rating, the more significant the threat. The challenge to this approach is the unexpected event. Sadly, as we saw on 9/11, threats are not always predicable. Table 12.1 presents threat assessments that take into account past occurrences.

TABLE 12.1 Threat Assessments: Historical

Threat Categories	Threat	Description	Likelihood Scale 1–5 [5=highest]	Impact Scale 1–5 [5=highest]	Impact Description	Inherent Risk (L*I)
Environmental	Wildfire	Wildfire in 2010 consumed 15,000 acres, approximately 50 miles northwest of HQ	4	5	Campus fire.	20 HIGH
Service provider dependency	Disruption of Internet connectivity	In 2012 and 2013, multiple periods of ISP downtime or extreme latency occurred.	4	5	Disruption of external mail, VPN connectivity, and cloud-based applications.	20 HIGH

Threat Categories	**Threat**	**Description**	**Likelihood** **Scale 1–5** [5=highest]	**Impact** **Scale 1–5** [5=highest]	**Impact Description**	**Inherent Risk** **(L*I)**
Service provider dependency	Brownouts	Summer temperatures and corresponding air conditioning usage consistently results in brief periods of low power.	3	5	Power fluctuations have the potential to damage equipment.	15 MED
Location	Flood	Flash flooding is an annual occurrence on Highway 16.	5	2	Campus not affected; however, deliveries and personnel may be.	10 LOW

What Is a Business Continuity Risk Assessment?

The business continuity threat assessment identifies the most likely and significant business continuity–related threats to the organization. The ***business continuity risk assessment*** evaluates the sufficiency of controls to prevent a threat from occurring or to minimize its impact. The outcome is the residual risk associated with each threat. The residual risk level provides management with an accurate portrayal of what happens if the threat is exercised under current conditions.

In a best-case scenario, the residual risk is within organizational tolerance. If the residual risk is not within tolerance, the organization must decide to take action to lower the risk level, approve the risk, or share the risk. Table 12.2 illustrates risk assessment considerations for the specific threat of a wildfire. The actual process and calculations used should mirror the organizational risk assessment methodology.

TABLE 12.2 Sample Wildfire Risk Assessment

Threat	Area Wildfires Resulting in Personnel Evacuation and Potential Destruction
Inherent Risk	High [as determined by the threat assessment]
Control Assessment	
Physical Controls	Fire berm around the campus. Contract with local firm for quarterly removal of flammable shrubs, leaves, dead limbs, and twigs within a 1,000-foot zone.

Building Controls	Fireproof construction. Sensor alarms with Fire Department (FD) notification. Fire and smoke sensors and sprinklers through the building. Fire safety maps throughout the building. Lighted emergency exits. No outside flammable substances stored near the building.
Data Center Controls	Sensor alarms with FD notification. Clean agent fire suppression system. Water mist system.
Personnel Controls	Evacuation plans. Fire drills conducted quarterly.
Technology Controls	Secondary data center 300 miles from primary campus. Near-time data replication. Secondary data center can support 200 concurrent remote users.
Financial Controls	Fire and hazard insurance policy. Business disruption insurance policy.
Control Assessment	Satisfactory.
Identified Vulnerabilities	Gas-powered generator. Gas fumes are combustible.
Residual Risk	Elevated.
Risk Reduction Recommendation	Replace gas-powered generator with diesel-powered generator.

Lowering the risk level requires the organization to implement additional controls and safeguards and/or to modify existing ones. In general, preventative or mitigating controls that deter, detect, and/or reduce disruption and impact are preferable to contingency procedures or recovery activities. As new technologies become available, preventative controls should be reevaluated and recovery strategies modified. The widespread adoption of virtualization as a preventative control is a good example of how technological innovation can influence business continuity planning.

Approving the risk implies that the organization is willing to assume the level of risk even though it is not within an acceptable range. As we discussed in Chapter 4, approving elevated or severe risk level is an executive-level decision. The decision may be based on cost, market conditions, external pressures, or a willingness to play the odds.

Risk sharing is when the risk (and consequences) are distributed among two or more parties. Examples are outsourcing and insurance.

What Is a Business Impact Assessment?

The objective of a ***business impact assessment (BIA)*** is to identify *essential* services/processes and recovery timeframes. In business continuity planning, *essential* means that the absence of, or disruption of, would result in significant, irrecoverable, or irreparable harm to the organization, employees, business partners, constituents, community, or country. Participants in the BIA process often incorrectly equate important with essential. There are a number of very important organization activities, such as marketing, recruiting, and auditing, that can be suspended in a disaster situation without impacting the viability of the organization, endangering constituents, or violating the law. On the other hand, there are mundane services such as maintaining an ATM cash dispenser that may be critical in a regional disaster. The key is to stay focused on the services required in the hours and days after a disaster strikes.

A business impact analysis is a multistep collaborative activity that should include business process owners, stakeholders, and corporate officers:

- **Step 1:** Identify essential business services and processes.
- **Step 1A:** Determine the maximum tolerable downtime for each service.
- **Step 2:** Identify supporting infrastructure, information systems, and dependencies.
- **Step 2A:** Determine recovery time objectives and recovery point objectives.
- **Step 3:** Compare to current recovery capability.
- **Step 3A:** Document the gap between desired and current capabilities.
- **Step 4:** Have stakeholders review the report for accuracy.
- **Step 5:** Present the BIA to management for approval.

As noted in the previous steps, the BIA process incorporates three metrics:

- The ***maximum tolerable downtime (MTD***) is the total length of time an essential *business function* can be unavailable without causing significant harm to the business.
- The ***recovery time objective (RTO)*** is the maximum amount of time a *system resource* can be unavailable before there is an unacceptable impact on other system resources or business processes.
- The ***recovery point objective (RPO)*** represents the point in time, prior to a disruption or system outage, that data can be recovered (in other words, the acceptable data loss).

In a perfect world, every essential system would be either redundant or available for immediate or near-time recovery. In reality, no organization has unlimited financial resources. The MTD, RTO, and RPO are useful in determining the optimum recovery investment and ancillary plans.

The outcome of a business impact analysis is a prioritized matrix of services, the required infrastructure, information systems, and dependencies for each service, recovery objectives, assessment of capabilities, and delta between the current and desired state. This information is then used by executive management to make investment decisions and to guide the development of disaster recovery and business contingency plans and procedures. Assuming an organization rated “Customer Communications” as an essential business process or service, Table 12.3 illustrates the components of a BIA.

TABLE 12.3 Business Impact Assessment: Customer Communications

Essential Business Process or Service: Customer Communications

Delivery Channels	Call Center	Website	Email
Required Infrastructure	Voice circuits. Wide area network power.	Internet access.	Internet access. Wide area network power.
Required Devices/ Information Systems	IP phone system. Call center system.	Hosted externally.	Email system, including email application servers and gateway filters. Authentication servers.
Third-Party Dependencies	Telco voice circuits.	Web hosting company. Internet Service provider (ISP).	DNS propagation.
Maximum Tolerable Downtime (MTD)	5 minutes.	Need to update the site within 60 minutes.	60 minutes.
Recovery Time Objective (RTO)	Immediate.	30 minutes.	45 minutes.
Recovery Point Objective (RPO)	12 hours for historical data.	24 hours for website content.	No acceptable data loss.
Current Capability	All calls will be automatically rerouted to the secondary data center. Redundant call center system located at secondary data center. Statistical data can be restored from backups. Data is replicated every 4 hours.	Localized disaster would not impact the website.	Redundant fully replicated email infrastructure located at the secondary data center. Assuming access to the secondary data center, external email will not be impacted. Incoming email will be delayed approximately 15 minutes, which is the time it takes for an MX record to be updated.
Identified Issues/Points of Failure	Call center staff is located at the primary location. Relocation will take a minimum of 8 hours.	Administrative access (required for updating) is restricted to specific IP addresses. Updating the access list is a third-party function. SLA is 30 minutes.	If the primary campus is available, the impact is minimal. If the primary campus is unavailable, only those users with remote access capability will be able to utilize email.
Capability Delta	755 minutes	0	+ 30 minutes
Data Loss Delta	0	0	0

In Practice

Business Impact Assessment

Synopsis: Require and assign responsibility for an annual BIA.

Policy Statement:

- The Chief Operating Office is responsible for scheduling an enterprise-wide annual BIA. System owner participation is required.
- The BIA will identify *essential* services and processes. *Essential* is defined as meeting one or more of the following criteria:
  - Required by law, regulation, or contractual obligation.
  - Disruption would be a threat to public safety.
  - Disruption would result in impact to the health and well-being of employees.
  - Disruption would result in irreparable harm to customers or business partners.
  - Disruption would result in significant or unrecoverable financial loss.
- For each essential service and/or process, the maximum tolerable downtime (MTD) will be documented. The MTD is the total length of time an essential function or process can be unavailable without causing significant harm to the business.
- For each essential service and/or process, supporting infrastructure, devices/information systems, and dependencies will be identified.
- Recovery time objectives (RTOs) and recovery point objectives (RPOs) for supporting infrastructure and devices/information systems will be documented.
- Current capability and capability delta will be identified. Deviations that put the organization at risk must be reported to the Board of Directors.
- The Chief Operating Officer, the Chief Information Officer, and the Business Continuity Team are jointly responsible for aligning the BIA outcome with the business continuity plan.

The Business Continuity Plan

The objective of business continuity planning is to ensure that organizations have the capability to respond to and recover from disaster situations. ***Response plans*** focus on the initial and near-term response and include such elements as authority, plan activation, notification, communication, evacuation, relocation, coordination with public authorities, and security. ***Contingency plans*** focus on immediate, near-term, and short-term alternate workforce and business processes. ***Recovery plans*** focus on the immediate, near-term, and short-term recovery of information systems, infrastructure, and facilities. ***Resumption plans*** guide the organization back to normalcy. Taken as a whole, this plan is referred to as the ***business continuity plan (BCP)*** or as the ***continuity of operations plan (COOP)***. The discipline is referred to as ***business continuity management***.

In Practice

Business Continuity Plan Policy

Synopsis: Require the organization to have a business continuity plan.

Policy Statement:

- The company's business continuity strategy will be documented in a business continuity plan. The plan will include plans, procedures, and ancillary documentation related to emergency preparedness, disaster preparation, response, contingency operations, recovery, resumption, training, testing, and plan maintenance.

Roles and Responsibilities

If we consider that the objective of business continuity management is to keep the business in business, it stands to reason that the responsibility must be distributed throughout the organization. Business continuity management involves the entire organization, from the Board member who approves the policy to the employee who carefully follows a related procedure. Depending on the size and complexity of the organizations as well as the nature of disaster, third parties such as public health and safety personnel, insurance representatives, legal counsel, service providers, and government agencies may all have a role to play. Business continuity responsibilities can be categorized as governance, operational, and tactical.

Governance

Governance is a continuing process in which diverse objectives, competing interests, and a range of ideas are evaluated and ultimately binding decisions are made and supported. It is the responsibility of the Board of Directors (or equivalent) to provide oversight and guidance, authorize business continuity management–related policy, and be legally accountable for the actions of the organization.

Executive management is expected to provide leadership, demonstrate commitment, allocate budget, and devote resources to the development and continued upkeep of the BCP. In an emergency, they declare a disaster, activate the plan, and support the Business Continuity Team.

Operational Management

When disaster strikes, quick mobilization is essential to mitigate damages. It is imperative that there be designated leadership with the authority to act quickly. This is the primary role of the ***Business Continuity Team (BCT)***, which is vested by the Board of Directors with the authority to make decisions related to disaster preparation, response, and recovery. BCT membership should represent a cross-section of the organization, including senior management, physical security, information technology (IT), human resources (HR), marketing/communications, information security, and business units. In concert, the team is responsible for the development, maintenance, testing, and updating of all related plans. The BCT may create subteams and assign responsibilities. Because the BCT will operate in unpredictable situations, second-in-command personnel should be trained and ready to assume their position. Once executive management has declared a disaster and activated the plan, the BCT is responsible for assessing damage, managing the response, communications, continuity, and recovery activities, and providing status updates to executive management. It’s also tasked with providing a post-disaster assessment of recovery and response efforts.

Tactical Activities

Tactical responsibilities are distributed throughout an enterprise. Depending on the size of the organization, some of these responsibilities may be consolidated. Unfortunately, it is all too common to encounter organizations that view the IT department as the owner of the business continuity process and expect IT to “take care of it.” Although it is true that IT is a vital participant, business continuity management, as suggested by the following list, is an organization responsibility:

- The *IT department* is responsible for designing and supporting resilience systems and for the recovery of information and information systems in a disaster situation.
- *Department managers* are responsible for defining the operational needs of their department and for creating and maintaining functional departmental contingency procedures.
- The *HR department* is responsible for the communication with and welfare of personnel and provides emergency-related services and assistance.
- The *marketing or communications department* is responsible for crafting and releasing official statements, communicating with the media, as well as managing internal communication include updates.
- The *purchasing department* is responsible for expediently ordering necessary supplies and equipment.
- The *training department* is responsible for delivering business continuity–related training and ancillary materials.
- The *internal audit department* audits the BCP and procedures and reports its findings to executive management. The audit satisfies the best practice requirements of separation of duties and oversight.

In Practice

Business Continuity Management Policy

Synopsis: Assign business continuity management responsibilities.

Policy Statement:

- The Board of Directors is responsible for authorizing the business continuity plan. Reference to the business continuity plan is inclusive of plans, procedures, and ancillary documentation related to disaster preparation, response, contingency operations, recovery, resumption, training, testing, and plan maintenance. The Board must be appraised on a timely basis of any material changes to the business continuity strategy.
- The Chief Operating Officer or designee is responsible for the development, maintenance, and management of the business continuity strategy and plan.
- The Chief Financial Officer will include business continuity expenses in the annual operating budget.
- The Office of Information Technology is responsible for designing and supporting resilient systems and for the recovery of information and information systems in a disaster situation.
- Senior managers are responsible for defining the operational needs of their departments and for creating and maintaining functional departmental contingency procedures.
- The Chief Operating Officer will appoint the Business Continuity Team chairperson. The chairperson will appoint members of the Business Continuity Team. The team must include representatives of key functional areas, including but not limited to operations, communications, finance, IT, information security, physical security, and facilities management. Team members are responsible for designating backups to serve in their absence.
- Business Continuity Team responsibilities include active participation in business continuity preparation, response, recovery, and resumption activities. At its discretion, the Business Continuity team may create subteams and assign responsibilities.
- The President/CEO has authority to declare an emergency, activate the plan, and contact/assemble the Business Continuity Team. In her absence, the COO has the authority to declare an emergency, activate the plan, and contact/assemble the Business Continuity Team. In his absence, the CFO has the authority to declare an emergency, activate the plan, and contact/assemble the Business Continuity Team. If none of the above listed are available, the Business Continuity Team chair in consultation with the Chairman of the Board of Directors has the authority to declare an emergency, activate the plan, and contact/assemble the Business Continuity Team.
- The Business Continuity Team will be the authoritative body during emergency response and recovery periods. Officers and employees will continue to conduct the affairs of the company under the guidance of the team leadership, except in matters that by statute require specific approval of the Board of Directors, or to conform to any governmental directives.

FYI: Business Continuity Management Education and Certification

DRI International (originally Disaster Recovery Institute International) was founded in 1988 as a nonprofit organization with the mission to make the world prepared. As the global education and certification body in business continuity and disaster recovery planning, DRI International sets the standard for professionalism. There are more than 11,000 active certified professionals worldwide. Continuity Professional certifications include Associate Business Continuity Professional (ABCP), Certified Functional Continuity Professional (CFCP), Certified Business Continuity Professional (CBCP), and Master Business Continuity Professional (MBCP). In addition, professionals may choose to specialize in audit, public sector, or healthcare. Learn more at www.drii.org.

Disaster Response Plans

What happens in those initial moments following a disaster that has both an immediate impact and a noteworthy ripple effect. Disaster response can be either chaotic or orderly. The difference between these scenarios is established procedures and responsibilities. Think back to elementary school days. Hopefully, you never experienced a fire at your school. But if you had, chances are that everyone would have evacuated the building safely. Why? Teachers and staff had specific assignments. Evacuation routes were mapped out. Students were taught not to panic, to line up single file, to follow a leader, and to gather at a specific location. All of these procedures and roles were reinforced through regularly scheduled fire drills. Similarly, organizations that have prepared for a disaster are able to focus on three immediate response goals:

1. Protecting the health and safety of employees, customers, first responders, and the public at large.
2. Minimizing damage to property and the environment.
3. Evaluating the situation and determining next steps.

The response plan should define the organizational structure, roles, and responsibilities, designated command and control, communications, and alternate work sites. Ancillary to the disaster response plan is the occupant emergency plan and procedures for immediate personnel safety. This plan is maintained separately because it may be used in nondisaster situations.

Organizational Structure

An orderly response requires both disciplined leadership and acknowledgement of who is in charge. First and foremost, it is incumbent upon everyone to follow the instructions of first responders and public safety officials. Board-approved policy should vest corporate officers or executive management with the authority to declare an emergency and activate the plan. In a disaster situation, the organizational structure and/or chain of command may be affected by injury, death, travel restrictions, or personal circumstances. It is important to have a clearly defined Board-approved succession plan.

For decisions pertaining to the response, continuity, and recovery effort, the BCT is generally the authoritative body. Because this is a departure from normal operating conditions, it is critical that executive management publicly support the authority of the BCT and that employees know who is in charge.

Command and Control Centers

Upon declaration of a disaster and the activation of the BCP, all BCT members should report to a designated command and control center. Primary and alternate ***command and control centers*** (sometimes referred to as "war rooms") are predetermined locations equipped to support the work of the BCT. A conference room, a training room, or even a large office can quickly be transformed into a command and control center. The command and control center is initially used to direct operations, and then may be used as a meeting center until normal business operations resume. At a minimum, the command and control center should be pre-stocked with the BCP manuals, tables, chairs, whiteboards, phones, surge strips, and mobile device power cords. If available (and operational), having voice and video conferencing equipment on hand serves to facilitate communication. All BCT members should have directions to the location, keys, and access codes.

Communication

A disaster may occur with little or no advance warning. The importance of the capability to quickly alert and account for employees, service providers, and first responders cannot be overstated. Every organization should have an ***occupant emergency plan (OEP)***, which describes evacuation and shelter-in-place procedures in the event of a threat or incident to the health and safety of personnel. Such events include fire, bomb threat, chemical release, domestic violence in the workplace, or medical emergency. The OEP is distinct from the BCP and is often maintained by either the HR department or facilities management.

The business continuity response plan must assign responsibility for both internal and external communications and include instructions for using a variety of communications channels. To prevent miscommunication, a designated communications liaison and spokespersons should be appointed. All public statements should be authorized by the BCT. Employees should be instructed that all media requests and questions be referred to the designated spokesperson without comment (on or off the record). The widespread use of social media is both a blessing and a curse. Social media can be used to quickly disseminate information and misinformation. Particularly in an evolving situation, employees may not have all the facts and/or may inadvertently disclose confidential information; they should be strongly discouraged from posting any information about the event on personal social media accounts.

Relocation Strategies

In cases of natural, environmental, or physical disaster, relocation of critical business functions may be necessary. Relocation strategies need to consider both delivery and operational business functions. *Delivery functions* provide service or product to the customer. An example would be the teller line at a bank or a customer call center. *Operational business functions* provide the core infrastructure of the organization. They include accounting, marketing, HR, office services, security, and IT. It may not be practical to consider relocating all staff. The relocation plan should consider staffing levels for essential services, space considerations, utility and environmental needs, transportation, and logistics. Telecommuting, including mobile device access, may minimize personnel relocation requirements. Options for alternate operational locations include hot, warm, cold, and mobile sites. Alternates sites may be owned, leased, or even borrowed. Organizations that have multiple operational sites may be able to redirect the workload to a location that has not been impacted by the disaster situation.

- A ***hot site*** is a location that is fully operational and ready to move into; it has been configured with redundant hardware, software, and communications capability. Data has been replicated to the hot site on a real-time or near-time basis.
- A ***warm site*** is an environmentally conditioned workspace that is partially equipped with information systems and telecommunications equipment to support relocated operations. Computers and devices located at warm sites need to be configured and brought online. Data needs to be restored.
- A ***cold site*** is a backup facility that has power, HVAC, and secure access. There is no staged equipment.
- ***Mobile sites*** are self-contained units. The units are provided by a third-party and generally arrive equipped with the required hardware, software, and peripherals. Data need to be restored.

In addition to the previous options, it may be possible to offload operations to service bureaus or outsource operations to third parties.

In Practice

Emergency Response Plan Policy

Synopsis: Ensure that the organization is prepared to respond to an emergency situation.

Policy Statement:

- The Chief Operating Officer is responsible for developing and maintaining the emergency response plan. The emergency response plan is a component of the enterprise business continuity plan.
- The objective of the emergency response plan is to protect the health and safety of employees, customers, first responders, and the public at large, minimizing damage to property and the environment, and set in motion response, contingency, and recovery operations.
- The emergency response plan must, at a minimum, address organizational alerts and notification, disaster declaration, internal and external communication channels, command and control centers, relocation options, and decision making authority.

- Ancillary to the response plan are OEPs and the crisis communication plan (CCP). Both plans may be utilized in conjunction with and/or referenced by the response plan.
  - The Office of Human Resources is responsible for maintaining the OEP.
  - The Office of Communications and Marketing is responsible for maintaining a CCP.
- Personnel responsible for response operations must receive appropriate training.
- Response plans and procedures must be audited in accordance with the schedule set forth by the Business Continuity Team.
- Response procedures must be tested in accordance with the schedule set forth by the Business Continuity Team.

Operational Contingency Plans

Operational contingency plans address how an organization's essential business processes will be delivered during the recovery period. Let's consider some examples:

- Physical access to facilities at a maximum-security prison is regulated by a biometric fingerprint access control system. The access control system is managed and monitored by an information system. The back-end information system becomes unavailable due to power loss. The business contingency procedure would address an alternate method to lock and unlock doors. This may be a physical key or perhaps an access code. In either case, knowing where the key is or what the code is would be essential to operations.

- A financial institution offers its customers the option of telephone banking services. Due to a fire, the telebanking phone system is not operational. Contingency procedures would address rerouting telebanking calls to customer service and ensuring that the customer service representatives (CSRs) could service the customers or at the very least provide information while the telebanking system is being recovered.

- A federal agency is forced to vacate its premises due to a biochemical threat. The agency receives and processes unemployment claims. Its most critical task is producing unemployment checks based on the claims. Unemployed individuals depend on receiving these payments in a timely manner. Business contingency procedures address alternate methods to accept and process claims as well as to print and distribute checks. Procedures may include notifying recipients by phone that payments are delayed, estimating payments based on the previous week's claims, and/or coordinating with another agency for processing and postal services.

Operational contingency plans and procedures are developed at the departmental level. They are the responsibility of the business process owner.

Operational Contingency Procedures

Operational contingency documentation should follow the same form as standard operating procedures. As with standard operating procedures, ***operational contingency operating procedures*** are instructions that should be understandable to everyone who may need to use them. They should be written as simply as possible. It is best to use short, direct sentences so that the reader can easily understand the procedure. Chapter 8, "Communications and Operations Security," introduced four formats for writing procedural documentation: simple step, hierarchical, graphic, and flowchart. These same formats are recommended for writing operational contingency operating procedures.

In Practice

Operational Contingency Plan Policy

Synopsis: Ensure that the organization can continue to provide essential services during the recovery period.

Policy Statement:

- Business process owners are responsible for developing and maintaining operational contingency plans. Operational contingency plans are a component of the enterprise business continuity plan.
- The operational contingency plans must include strategies and procedures for providing essential services as determined by the business impact assessment during the recovery operations.
- The amount of procedural detail required should be enough that competent personnel familiar with the service or process could perform the alternate operation.
- External system dependencies and relevant contractual agreements must be reflected in the contingency plan.
- Personnel responsible for contingency operations must receive appropriate training.
- Contingency plans and procedures must be audited in accordance with the schedule set forth by the Business Continuity Team.
- Contingency procedures must be tested in accordance with the schedule set forth by the Business Continuity Team.

The Disaster Recovery Phase

In the ***disaster recovery phase***, the organization begins the process of restoring or replacing damaged infrastructure, information systems, and facilities. Recovery activities can range from immediate failover to redundant systems to the significantly longer process of procuring equipment, restoring data, and potentially rebuilding facilities. Regardless of the strategy employed, it is critical that procedures have been documented and tested. Priorities for recovery operations should be consistent with the results of the business impact analysis.

Developing recovery plans and procedures can be a daunting task. A proven successful approach is to break the plan down into categories and assign responsibilities at the operational level, such as mainframe, network, communications, infrastructure, and facilities.

- *Mainframe recovery* is specific to the restoration a mainframe computer (or equivalent capability) and corresponding data processing.
- *Network recovery* is specific to information systems (servers, workstations, mobile devices, applications, data stores, and supporting utilities) and includes the restoration of functionality and data.
- *Communications recovery* encompasses internal and external transmission systems, including local area network (LAN), wide area network (WAN), data circuits (T1, T3, MPLS), and Internet connectivity. Included in this category are connectivity devices such as switches, routers, firewalls, and IDSs.
- *Infrastructure recovery* encompasses those systems providing a general operating environment, including environmental and physical controls.
- *Facilities recovery* addresses the need to rebuild, renovate, or relocate the physical plant.

The criticality and priority determined by the business impact analysis provides the framework for choosing the appropriate strategy and level of investment.

Recovery Procedures

A disaster is not the time to figure out how to recover or restore a system, nor is it the time to determine inventory or search for vendor contacts. All of these items need to be addressed beforehand and documented in recovery procedures and ancillary files. Recovery processes can be very technical. The procedures should explain in a logical progression, what needs to be done, where it needs to be done, and how it needs to be done. Procedures may reference other documents. Table 12.4 illustrates a recovery procedure for an Active Directory domain controller.

TABLE 12.4 Active Directory Domain Controller Recovery Procedure

Active Directory Domain Controller Recovery	
Support Phone Numbers	HP Support: 800-888-8888 Microsoft Technical Support ■ Regular Support: 888-888-9999 ■ Business Critical: 888-888-7777
General Information	Active Directory domain controllers provide authentication, DNS, and DHCP services. If a domain controller fails, the remaining domain controllers will be able to authenticate user accounts, provide DNS resolution, and assign dynamic addresses. Note: Users may notice a degradation of service.

Configuration Information	There are four Windows Server domain controllers: ■ Two are located at the data center in rack 7G. ■ One is located in the Building A data closet rack. It is the second device from the top. ■ One is located in the Building B data closet rack. It is the fourth device from the top. There are five FSMO roles that are server specific: schema master, domain naming master, PDC emulator, RID master, and infrastructure master. ■ Reference/recovery/server_roles.xls for server assignments. ■ For more information on FMSO roles, refer to http://support.microsoft.com/kb/324801.
Recovery/ Resumption Instructions	1. If a domain controller fails, its objects and attributes will have to be removed from the Active Directory, and any FSMO roles that it held would have to be transferred to another domain controller. Follow the steps in http://support.microsoft.com/kb/216498 to remove the data. 2. After the failed domain controller has been removed from Active Directory, a replacement can be built. A virtual machine (VM) could be used to replace a (physical) server. ■ Create a cloned VM from a template. ■ Assign it the host name and static IP address of the failed domain controller. ■ Patch the new server and install antivirus. ■ From a run command, type DCPROMO to promote the member server to be a DC. 3. Accept the default setting and follow the prompts to complete the promotion. 4. Configure DNS for zone transfers and set the forwarders. ■ Reference/recovery/DNS_recovery_procedures for DNS configuration instructions. 5. Configure DHCP scope information and restore assignments. ■ Reference/recovery/DHCP_recovery_procedures for DHCP configuration instructions.

The key to disaster recovery is the ability to respond using validated, maintained, and tested procedures. All recovery procedures should be reviewed annually. Planning for recovery is a component of the systems development lifecycle (SDLC) process.

Service Provider Dependencies

Recovery plans often depend on vendors to provide services, equipment, facilities, and personnel. This reliance should be reflected in contractual service agreements. ***Service level agreements (SLAs)*** should specify how quickly a vendor must respond, the type and quantity of replacement equipment guaranteed to be available, personnel and facility availability, and the status of the organization in the event of a major disaster involving multiple vendor clients. Service agreements should be referenced in the procedure as well as contact information, agreement numbers, and authorization requirements. Service provider dependencies should be included in the annual testing.

In Practice

Disaster Recovery Plan Policy

Synopsis: Ensure that the organization can recover infrastructure, systems, and facilities damaged during a disaster.

Policy Statement:

- The Office of Information Technology and the Office of Facilities Management are responsible for their respective disaster recovery plans. Disaster recovery plans are a component of the enterprise business continuity plan.
- The disaster recovery plan must include recovery strategies and procedures for systems and facilities as determined by the business impact assessment.
- Modifications to the recovery plan must be approved by the Chief Operating Officer.
- The amount of procedural detail required should be enough that competent personnel familiar with the environment could perform the recovery operation.
- External system dependencies and relevant contractual agreements must be reflected in the recovery plan.
- Personnel responsible for recovery operations must receive appropriate training.
- Recovery plans and procedures must be audited in accordance with the schedule set forth by the Business Continuity Team.
- Recovery procedures must be testing in accordance with the schedule set forth by the Business Continuity Team.

The Resumption Phase

The objective of the ***resumption phase*** is to transition to normal operations. Two major activities are associated with this phase—validation of successful recovery and deactivation of the BCP.

Validation is the process of verifying that recovered systems are operating correctly and that data integrity has been confirmed. Validation should be the final step of every recovery procedure.

Deactivation is the official notification that the organization is no longer operating in emergency or disaster mode. At this point, the BCT relinquishes authority, and normal operating procedures are reinstated. Once the dust settles, figuratively and literally, an after-action report with lessons learned should be documented by the BCT. The BCP should be reviewed and revised based on the findings and recommendations of the BCT.

Plan Testing and Maintenance

A BCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability. NIST SP 800-84: Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events.

Why Is Testing Important?

It would be hard to overstate the importance of testing. Until tested, plans and procedures are purely theoretical. The objective of a testing program is to ensure that plans and procedures are accurate, relevant, and operable under adverse conditions. As important as demonstrating success is uncovering inadequacies. The worst time to find out that your plans were incomplete, outdated, or just plain wrong is in the midst of a disaster. The extent and complexity of the testing program should be commensurate with the criticality of the function or system. Prior to testing, a test plan should be developed that details the test objective, type of test, success criteria, and participants.

In addition to procedures being tested, the BCP should be audited. At a minimum, testing exercises and audits should be conducted annually. The results of both should be provided to the Board of Directors.

Testing Methodologies

There are three standard testing methodologies: tabletop exercises, functional exercises, and full-scale testing. ***Tabletop exercises*** can be conducted as structured reviews or simulations*:*

- A ***structured review*** focuses on a specific procedure or set of procedures. Representatives from each functional area participate in a systematic walkthrough of the procedures with the goal of verifying accuracy and completeness. A structured review can also be used as a training exercise with the objective of familiarization.
- A tabletop ***simulation*** focuses on participant readiness. A facilitator presents a scenario and asks the exercise participants' questions related to the scenario, including decisions to be made, procedures to use, roles, responsibilities, timeframes, and expectations. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

Functional exercises allow personnel to validate plans, procedures, resource availability, and participant readiness. Functional exercises are scenario driven and limited in scope, such as the failure of a critical business function or a specific hazard scenario. Functional exercises can be conducted in either a parallel or production environment.

Full-scale testing is conducted at the enterprise level. Based on a specific scenario, the business operates as if a disaster was declared. Normal operations are suspended. Recovery and contingency plans and procedures are implemented. Full-scale testing can be expensive and risky. It is, however, the most accurate test of plans and procedures.

Audits

A ***business continuity plan audit*** is an evaluation of how the business continuity program in its entirety is being managed. This includes policy, governance, assessments, documentation, testing, and maintenance. Audits are conducted by personnel independent of the response, contingency, or recovery efforts. Auditors will look at the quality and effectiveness of the organization's BCP process, and determine whether the testing program is sufficient. At a minimum, you can anticipate they will ask the following questions:

- Is there a written business continuity policy and plan?
- Has the business continuity policy and plan been approved by the Board of Directors?
- How often is it reviewed and/or reauthorized?
- How often is a BIA conducted? By whom?
- Who is on the BCT?
- What training have they had?
- What training has the user community had?
- Is there a written test plan?
- How often is the plan tested?
- Are the results documented?
- If third parties are involved, what is the process for testing/verifying their procedures?
- Who is responsible for maintaining the plan?

As with all examinations and audits, independence must be maintained. Examiners and auditors must not be connected to the management or maintenance of related policies, plans, procedures, training, or testing.

Plan Maintenance

BCPs must stay in synch with organizational and personnel changes. At a minimum, on an annual basis, roles and responsibilities, including BCT membership, should be revisited, a BIA conducted, and recovery and contingency plans evaluated. Aside from the annual review, the BCP may need to be updated due to changes in regulatory requirements, technology, and the threat landscape.

FYI: Regulatory Expectations

The best way to know what to expect from an audit is to be privy to audit work papers. Fortunately, one of the best set of work papers is in the public domain. The Federal Financial Institutions Examination Council (FFIEC) develops and publishes guides and audit work papers for use by field examiners in financial institution regulatory agencies. These resources are found in the *FFIEC Information Technology Examination Handbook InfoBase*. The handbook is available to the public and can be downloaded from the FFIEC website at www.ffiec.gov.

In Practice

Business Continuity Testing and Maintenance Policy

Synopsis: Codify testing and maintenance requirements and responsibility.

Policy Statement:

- Reference to the business continuity plan is inclusive of plans, procedures, and ancillary documentation related to disaster preparation, response, contingency operations, recovery, resumption, training, testing, and plan maintenance.
- The Chief Operating Officer or designee is responsible for maintenance of the business continuity plan.
- The Chief Operating Officer or designee will conduct an annual review of the business continuity plan.
- The Business Continuity Team is responsible for publishing an annual testing schedule and managing the test plan. The Chief Operating Officer will report the results to the Board of Directors.
- Internal audit is tasked with managing and selecting an independent firm to conduct an annual audit of the business continuity plan. The independent audit firm will report the results to the Board of Directors or designated committee.

FYI: Small Business Note

A disaster situation can be particularly devastating to a small business, yet few are prepared. According to David Paulison, former executive director of the Federal Emergency Management Agency (FEMA), “Small businesses that don’t have a plan in place generally don’t survive after a disaster, whether it’s a flood or a tornado. We see that anywhere from 40–60 percent of those that are hit like that simply don’t come back to business.”

In response to the lack of preparedness, the Small Business Administration (SBA) has made available a number of general preparedness resources and specific disaster information designed to assist the small business community and support economic recovery.

General preparedness resources include an identifying critical business systems worksheet, creating a preparedness program template, and instructions on building a business disaster preparedness kit.

Specific disaster information includes hurricanes, winter weather, earthquakes, tornadoes, wildfires, floods, and cyber security.

The resources can be accessed at the following sites:

- www.sba.gov/content/disaster-preparedness#
- www.preparemybusiness.org/

Summary

A disaster is an event that results in damage or destruction, loss of life, or drastic change to the environment. Preparing for a disaster can make the difference between life and death, success or failure. Preparedness is a regulatory requirement for industry sectors deemed critical to national security. Not investing the time and effort required to face disruptions is negligent and the consequences severe.

A resilient organization is one that has the ability to quickly adapt and recover from known or unknown changes to the environment. The objective of business continuity planning is to ensure that organizations have the capability to respond to and recover from disaster situations. Response plans focus on the initial and near-term response and include such elements as authority, plan activation, notification, communication, evacuation, relocation, coordination with public authorities, and security. Contingency plans focus on immediate, near-term, and short-term alternate workforce and business processes. Recovery plans focus on the immediate, near-term, and short-term recovery of information systems, infrastructure, and facilities. Resumption plans guide the organization back to normalcy. Taken as a whole, this is referred to as the business continuity plan (BCP) or as the continuity of operations plan (COOP). The discipline is referred to as business continuity management.

The precursor to developing a BCP is assessing the threat environment and organizational risk as well as determining essential business services and processes. A business continuity threat assessment identifies viable threats and predicts the likelihood of occurrence. Threat modeling takes into account historical and predictive geographic, technological, physical, environmental, third-party, and industry factors.

A business continuity risk assessment evaluates the sufficiency of controls to prevent the threat from occurring or to minimize its impact. A business impact assessment (BIA) identifies essential services/processes and recovery timeframes. In BCP, *essential* means that the absence of, or disruption of, would result in significant, irrecoverable, or irreparable harm to the organization, employees, business partners, constituents, community, or country. The BIA process uses three prioritization metrics: MTD, recovery time objectives (RTOs), and recovery point objectives (RPOs). The MTD is the total length of time an essential business function can be unavailable without causing significant harm to the business. The RTO is the maximum amount of time a system resource can be unavailable before there is an unacceptable impact on other system resources or business process. The RPO represents the point in time, prior to a disruption or system outage, that data can be recovered; in other words, the acceptable data loss.

Business continuity management is a distributed responsibility. The Board of Directors or organizational equivalent is ultimately accountable for ensuring that the organization is prepared. It is the responsibility of executive management to ensure that threats are evaluated, impact to business processes recognized, and resources allocated. They are also charged with declaring a disaster and activating the BCP. The BCT, appointed by executive management, is expected to manage preparation and be the authoritative body in a declared disaster.

A BCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested and audited to ensure their operability. The plan in its entirety should be reviewed on a scheduled basis. It should be reauthorized annually by the Board of Directors or organizational equivalent.

Business Continuity Management policies include Emergency Preparedness, Business Impact Assessment, Business Continuity Management, Emergency Response Plan, Operational Contingency Plan, Disaster Recovery Plan, and Business Continuity Testing and Maintenance.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following terms best describes the primary objective of business continuity?

   A. Assurance

   B. Availability

   C. Accounting

   D. Authentication

2. Which of the following statements best describes a disaster?

   A. A disaster is a planned activity.

   B. A disaster is an isolated incident.

   C. A disaster is a significant disruption of normal business functions.

   D. A disaster is a change in management structure.

3. Flood, fire, and wind are examples of which type of threat?

   A. Malicious act

   B. Environmental

   C. Logistical

   D. Technical

4. Which of the following terms best describes the process of identifying viable threats and likelihood of occurrence?

   A. Risk assessment

   B. Threat assessment

   C. Likelihood assessment

   D. Impact assessment

5. Which of the following terms best describes the process of evaluating the sufficiency of controls?

   A. Risk assessment
   B. Threat assessment
   C. Likelihood assessment
   D. Impact assessment

6. Which of the following statements best describes the outcome of a BIA?

   A. A BIA generates RTOs.
   B. A BIA produces an organizational agreement on essential processes and services.
   C. A BIA identifies the gap between current and desired recovery capabilities.
   D. All of the above

7. An acceptable length of time a business function or process can be unavailable is known as _________________.

   A. maximum unavailability (MU)
   B. total acceptable time (TAT)
   C. maximum tolerable downtime (MTD)
   D. recovery time objective (RTO)

8. The recovery point objective (RPO) represents ____________.

   A. acceptable data loss
   B. acceptable processing time loss
   C. acceptable downtime
   D. None of the above

9. Recovery time objectives relate to which of the following?

   A. Business services
   B. Data restoration
   C. Information systems
   D. None of the above

10. Which of the following plans are included in a BCP?

- **A.** Resumption plans
- **B.** Response plans
- **C.** Contingency plans
- **D.** All of the above

11. Legal and regulatory accountability for an organization's preparedness is assigned to _______________.

- **A.** the BCT
- **B.** regulators
- **C.** the Board of Directors or organizational equivalent
- **D.** service providers

12. The authority to declare an emergency and activate the plan is owned by ____________.

- **A.** the BCT
- **B.** executive management
- **C.** the Board of Directors or organizational equivalent
- **D.** service providers

13. Which of the following plans include evacuation and in-shelter procedures?

- **A.** The fire drill plan
- **B.** The occupant emergency plan
- **C.** The business contingency plan
- **D.** A FEMA directive

14. Which of the following entities is responsible for the ongoing command of operations in the event of a disaster?

- **A.** First responders
- **B.** The BCT
- **C.** The Chairman of the Board
- **D.** The Information Security Officer

15. The designated location for the BCT operations is referred to as the ___________.

- **A.** BCT office
- **B.** hot site
- **C.** command and control center
- **D.** conference room

16. Contingency and recovery procedures should include a level of detail appropriate for which of the following entities?

- **A.** New hires or temporary employees
- **B.** Cross-trained personnel or service providers familiar with the organization
- **C.** Auditors
- **D.** Examiners

17. The BCT is tasked with all of the following activities *except* ___________.

- **A.** testing the plan
- **B.** managing the plan
- **C.** reporting to the command and control center
- **D.** auditing the plan

18. Which type of alternate data-processing facility is fully equipped with all resources required to maintain operations?

- **A.** Hot site
- **B.** Warm site
- **C.** Cold site
- **D.** Off site

19. Which type of alternate data-processing facility has power and HVAC but not equipment?

- **A.** Hot site
- **B.** Warm site
- **C.** Cold site
- **D.** Off site

20. Which of the following statements is true of the IT department's responsibilities?

    A. The IT department is responsible for restocking supplies.

    B. The IT department is responsible for recovery and resumption related to the information system and supporting infrastructure.

    C. The IT department is responsible for rebuilding facilities.

    D. The IT department is responsible for the release of updates to the press.

21. Which of the following statements best describes the primary objective of an organization's contingency plan?

    A. The primary objective of an organization's contingency plan is for the organization to become fully operational.

    B. The primary objective of an organization's contingency plan is for the organization to recover systems.

    C. The primary objective of an organization's contingency plan is for the organization to notify authorities.

    D. The primary objective of an organization's contingency plan is for the organization to continue to provide services.

22. Which of the following entities is responsible for developing, validating, and training personnel on operational contingency plans?

    A. Business process owners

    B. BCT

    C. Business managers

    D. Business associates

23. Validation and deactivation activities are part of __________.

    A. response

    B. contingency

    C. recovery

    D. resumption

24. Which of the following should *not* be included in service provider agreements?

    A. Response time

    B. Replacement equipment

    C. Priority of service

    D. Emergency passcodes

25. Plan maintenance includes which of the following?

- **A.** Testing and auditing
- **B.** Departmental review
- **C.** Updating and distribution
- **D.** All of the above

26. Structured walkthrough exercises are designed to validate _________.

- **A.** procedures
- **B.** strategy
- **C.** resources
- **D.** readiness

27. Tabletop simulation exercises are designed to validate __________.

- **A.** procedures
- **B.** strategy
- **C.** resources
- **D.** readiness

28. Which of the following entities should conduct BCP audits?

- **A.** The IT department
- **B.** The Office of Information Security
- **C.** Independent auditors
- **D.** The BCT

29. Which of the following organizations is the federal agency whose primary responsibility is to respond to disasters and assist with business recovery?

- **A.** Department of Homeland Security (DHS)
- **B.** American Red Cross (ARC)
- **C.** Federal Emergency Management Agency (FEMA)
- **D.** National Guard

30. Which term best describes organizations that have the ability to quickly adapt and recover from known or unknown changes to the environment?

- **A.** Accountable
- **B.** Resilient
- **C.** Compliant
- **D.** Vulnerable

EXERCISES

EXERCISE 12.1: Assessing Threats

1. Based on historical occurrences, identify three environmental or location-based threats to your campus or workplace.
2. Choose one of the three threats and document how often the threat has occurred in the past 20 years.
3. Describe the factors you would take into consideration in predicting the likelihood of a reoccurrence within the next five years.

EXERCISE 12.2: Analyzing an Occupant Emergency Response Plan

1. Locate a copy of the occupant emergency response plan (note that it may go by a different name, such as evacuation plan) for your campus or workplace. If you cannot locate one, use the Internet to locate one from another school or organization.
2. When was the plan last updated?
3. Summarize the key components of the plan. In your opinion, does the plan provide adequate instructions?

EXERCISE 12.3: Assessing the Training and Testing of an Occupant Emergency Response Plan

1. Locate a copy of the occupant emergency response plan (note that it may go by a different name, such as evacuation plan) for your campus or workplace. If you cannot locate one, use the Internet to locate one from another school or organization. If you completed Exercise 12.2, you may use the same plan.
2. What type of exercises would you recommend in order to test the occupant emergency response plan.
3. What type of training would you recommend in order to educate personnel regarding the occupant emergency response plan.
4. If you were auditing the occupant emergency response plan, what questions would you ask?

EXERCISE 12.4: Researching Alternative Processing Sites

1. A number of companies specialize in offering “hot site” solutions. Locate at least three companies that offer this service.
2. Create a matrix comparing and contrasting options such as technical support, available bandwidth, traffic redirection, managed security, and data center features (for example, power and connectivity and geographic location).
3. Recommend one of the sites. Be prepared to explain your recommendation.

EXERCISE 12.5: Researching the Federal Emergency Management Agency

1. Describe the FEMA resources available online to businesses to help them prepare for disasters.
2. Describe the FEMA resources available online to families to help them prepare for disasters.
3. What is FEMA Corps?

PROJECTS

PROJECT 12.1: Assessing Disruptions in Business Continuity

Disruption in service at a financial institution impacts both its customers and internal operations.

1. Listed here are various disruptions in banking service. Assign each event a rating of 1–5 (1 is the lowest, 5 is the highest) that best represents the impact on you (as the customer) and provide an explanation of your rating. Consider each event independently.

   A. ATM system unavailable, branches open.

   B. Closest local branch closed, others open.

   C. Internet banking unavailable, branches open.

   D. Core processing system unavailable, deposits accepted, withdrawals less than $100, other account information unavailable.

   E. Communications capabilities between branches disrupted, tellers work in off-line mode.

2. Listed here are the same disruptions in banking service. Assign each event a rating of 1–5 (1 is the lowest, 5 is the highest) that best represents the impact on the bank from a financial, operational, legal, or regulatory perspective and provide an explanation. Consider each event independently.

   A. ATM system unavailable, branches open.

   B. Closest local branch closed, others open.

   C. Internet banking unavailable, branches open.

   D. Core processing system unavailable, deposits accepted, withdrawals less than $100, other account information unavailable.

   E. Communications capabilities between branches disrupted, tellers work in off-line mode.

3. Describe how business continuity planners should reconcile the differences in impact upon a business and its customers.

PROJECT 12.2: **Evaluating Business Continuity Plans**

The objective of this project is to evaluate your school or employer's BCP. You will need to obtain a copy of your school or employer's BCP (it may be known as a disaster response plan). If you cannot locate a copy, use the Internet to locate one from another school or organization.

1. Identify the sections related to preparation, response, contingency, recovery, resumption, testing, and maintenance. Is anything missing?
2. Identify roles and responsibilities referenced in the plan.
3. Critique the plan in terms of clarity and ease of use.

PROJECT 12.3: **Assessing the impact of "the Cloud" on Business Continuity**

Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are changing how organizations design their technology environments.

1. How do IaaS and PaaS impact business continuity planning?
2. Have any of the cloud service providers (such as Google, Amazon, Rackspace, Savvis) experienced any major outages that would impact their customers?
3. Assuming an organization used the services of a cloud provider for business continuity services, explain the type of response, recovery, and continuity testing they could/should conduct.

Case Study

The Role of Social Media in a National Crisis

Without warning, at 2:49 p.m. on April 15, 2013, two pressure cooker bombs exploded near the finish line of the Boston Marathon. Three people were killed, hundreds injured, and countless lives affected. The Boston Police Department used social media, including Twitter (@bostonpolice), to communicate with the country that day and in the days that followed. According to *The Huffington Post* analysis of the event, "The police department's stream of tweets ended up being the best defense against misinformation and Bostonians' lifeline for communication about the men terrorizing their city. This single Twitter account, perhaps more than anything else on the Internet, memorialized the horror of the bombs and the joy of the capture in real time."

1. Document how social media was used as an emergency communication tool during the aftermath of the Boston Marathon bombing.
2. Make a recommendation as to whether businesses should use social media as a communications tool during a disaster situation. Be sure to include both pros and cons.
3. Would your answer be different if the assignment was to make a recommendation as to whether colleges and universities should adopt social media for communicating about a disaster? Why or why not?

References

Regulations Cited

"16 CFR Part 314: Standards for Safeguarding Customer Information; Final Rule, Federal Register," accessed 05/2013, http://ithandbook.ffiec.gov/media/resources/3337/joisafeguard_customer_info_final_rule.pdf.

"HIPAA Security Rule," official website of the Department of Health and Human Services, accessed 05/2013, www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

Executive Orders Cited

"Federal Continuity Directive-1," office website of FEMA, accessed 09/2103, www.fema.gov/guidance-directives.

"Presidential Decision Directive-63, Critical Infrastructure Protection," official website of the Government Printing Office, accessed 09/2013, www.gpo.gov/fdsys/granule/FR-1998-08-05/98-20865/content-detail.htm.

"Presidential Directive-51/Homeland Security Presidential Directive-20, National Continuity Policy," official website of FEMA, accessed 09/2103, www.fema.gov/guidance-directives.

"Presidential Directive HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection," official website of the Department of Homeland Security, accessed 05/2013, www.dhs.gov/homeland-security-presidential-directive-7#1.

Other References

"An Overview of U.S. Regulations Pertaining to Business Continuity White Paper," accessed 09/2013, www.geminare.com/pdf/U.S._Regulatory_Compliance_Overview.pdf.

Bell, Michael. "The Five Principles of Organizational Resilience," Gartner Group, January 7, 2002, accessed 09/2013, www.gartner.com/id=351410.

Bindley, Katherine. "Boston Police Twitter: How Cop Team Tweets Led City from Terror to Joy," April 26, 2013, accessed 9/2013, www.huffingtonpost.com/2013/04/26/boston-police-twitter-marathon_n_3157472.html.

"Business Testimonials: Aeneas," FEMA Ready, accessed 09/2013, /www.ready.gov/business/business-testimonials.

"Disaster Planning," official website of the SBA, accessed 09/2013, www.sba.gov/content/disaster-planning.

"Emergency Preparedness," official website of the U.S. Small Business Administration, accessed 09/2013, www.sba.gov/content/disaster-preparedness#.

"Hurricane Sandy," Wikipedia, accessed 09/2013, http://en.wikipedia.org/wiki/Hurricane_Sandy.

"Hurricane Sandy: Covering the Storm," *The New York Times*, November 6, 2012, accessed 09/2013, www.nytimes.com/interactive/2012/10/28/nyregion/hurricane-sandy.html?_r=0.

Kane, Gerald C. "What Can Managers Learn about Social Media from the Boston Marathon Bombings," *MIT Sloan Management Review*, April 25, 2013, accessed 09/2013, http://sloanreview.mit.edu/article/what-can-managers-learn-about-social-media-from-the-boston-marathon-bombing/.

MacDonald, Caroline. "Experts Say Small Firms Lag in Disaster Planning," Property Casualty 360°, November 11, 2009, accessed 09/2013, www.propertycasualty360.com/2009/11/11/experts-say-small-firms-lag-in-disaster-planning.

"National Disaster Recovery Framework," official website of FEMA, accessed 09/2013, www.fema.gov/national-disaster-recovery-framework.

"National Preparedness Guidelines, Department of Homeland Security, September 2007," accessed 09/2013, www.fema.gov.

"Preparedness Planning for Your Business," FEMA Ready, accessed 09/2013, www.ready.gov/business.

"Closing the Seams: Developing an integrated approach to health system disaster preparedness," PricewaterhouseCoopers' Health Research Institute, accessed 09/2013, www.pwc.com/us/en/healthcare/publications/closing-the-seams.jhtml.

Rogers, Simon. "The Boston Bombing: How journalists used Twitter to tell the story," Twitter Blog, July 20, 2013, accessed 09/2013, https://blog.twitter.com/2013/the-boston-bombing-how-journalists-used-twitter-to-tell-the-story.

Chapter 13

Regulatory Compliance for Financial Institutions

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Explain financial institution information security regulatory compliance requirements.
- Understand the components of a GLBA-compliant information security program.
- Prepare for a regulatory examination.
- Respond to the twin threats of personal identity theft and corporate account takeover.

Banks and credit unions provide an array of financial services. Although it may appear that money is their most valuable asset, the reality is that customer and transactional information is the heart of their business. Money is fungible and can be replaced. Protection of customer information is necessary to establish and maintain trust between the financial institution and the community it serves. More specifically, institutions have a responsibility to safeguard the privacy of individual consumers and protect them from harm, including fraud and identity theft. On a broader scale, the industry is responsible for maintaining the nation's financial services critical infrastructure.

In this chapter, we will examine the regulations applicable to the financial sector. We will focus on Title 5 Section 501(b) of the Gramm-Leach-Bliley Act (GLBA) and the corresponding interagency guidelines, Federal Trade Commission (FTC) Safeguards Act, and Financial Institutions Letters (FILS). Compliance with GLBA is mandatory. Noncompliance has significant penalties, including being forced to cease operations. As we examine the various regulations, we will look at how examiners assess compliance. We will conclude the chapter with a look at the most significant financial security issue of our time—personal and corporate identity theft—and the regulations that address this ever-growing problem.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 15 of ISO 27002:2013 is dedicated to the Compliance Management domain, which focuses on compliance with local, national, and international criminal and civil laws, regulatory or contractual obligations, intellectual property rights (IPRs), and copyrights.

Corresponding NIST guidance is provided in the following document:

- SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

The Gramm-Leach-Bliley Act (GLBA)

In a response to the massive bank failures of the Great Depression, the Banking Act of 1933 prohibited national and state banks from affiliating with securities companies. The specific provision is often referred to as the Glass-Steagall Act. Similar to the Glass-Steagall Act, the Bank Holding Company Act of 1956 prohibited banks from controlling a nonbank company. This act was amended by Congress in 1982 to further forbid banks from conducting general insurance underwriting or agency activities.

On November 11, 1999, the Glass-Steagall Act was repealed and the ***Gramm-Leach-Bliley Act (GLBA)*** was signed into law by President Bill Clinton. Also known as the ***Financial Modernization Act of 1999,*** GLBA effectively repealed the restrictions placed on banks during the six preceding decades, which prevented the merger of banks, stock brokerage companies, and insurance companies. Prior to GLBA, the insurance company that maintained health records was by law unrelated to the bank that financed mortgages and the brokerage house that traded stocks. Once merged, however, companies would have access to a cross-section of personal information. Using data-mining techniques, it is possible to build detailed customer and prospect profiles. Because of the potential for misuse of information, Title 5 of GLBA specifically addresses protecting both the privacy and the security of non-public personal information (NPPI).

- The ***Privacy Rule*** limits a financial institution's disclosure of NPPI to unaffiliated third parties, such as by selling the information to unaffiliated third parties. Subject to certain exceptions, the Privacy Rule prohibits disclosure of a consumer's NPPI to a nonaffiliated third party unless certain notice requirements are met and the consumer does not elect to prevent, or "opt out of," the disclosure. The Privacy Rule requires that privacy notices provided to customers and consumers describe the financial institution's policies and practices to protect the confidentiality and security of that information. It does *not* impose any other obligations with respect to safeguarding customers or their information.

- The ***Security Guidelines*** address safeguarding the confidentiality and security of customer NPPI and ensuring the proper disposal of customer NPPI. They are directed toward preventing or responding to foreseeable threats to, or unauthorized access or use of, that information.

Non-public personal information (NPPI) includes (but is not limited to) names, addresses, and phone numbers when linked to bank and credit card account numbers, income and credit histories, and social security numbers (SSNs). Regulatory language uses the terms *sensitive customer information* and *NPPI* interchangeably.

What Is a Financial Institution?

GLBA defines a ***financial institution*** as “Any institution the business of which is significantly engaged in financial activities as described in *Section 4(k) of the Bank Holding Company Act* (12 U.S.C. § 1843(k).” This broad definition means that the regulation applies to traditional financial institutions such as banks, credit unions, and investment firms as well as companies that offer financial products or services to customers. The net effect is that GLBA applies to automobile dealers, check-cashing businesses, consumer reporting agencies, credit card companies, credit counselors, data processors, debt collectors, educational institutions that provide financial aid, financial planners, insurance companies, loan brokers, mortgage brokers and lenders, real estate settlement service providers, and retail stores that issue credit cards.

Regulatory Oversight

All financial institutions that conduct business in the United States are subject to GLBA. The regulation gives authority to various agencies to administer and enforce the privacy and security provisions. Table 13.1 lists the agencies, their charges, and the applicable public law. By law, the agencies were required to work together to issue consistent and comparable rules to implement the Act’s privacy provision. In contrast, the agencies were tasked with independently establishing minimum-security standards as well as determining the type and severity of the penalties.

- The Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRS), Federal Deposit Insurance Corporation (FDIC), and Office of Thrift Supervision (OTS) jointly developed the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*. The final rule was published in the Federal Register on February 1, 2001, with an effective date of July 1, 2001.
- The National Credit Union Administration (NCUA) published their *Guidelines for Safeguarding Member Information* on January 30, 2001, with an effective date of July 1, 2001.
- The Securities and Exchange Commission (SEC) incorporated a safeguards rule as part of its Privacy of Consumer Financial Information June 2000 Final Rule.
- The FTC published their *Standards for Safeguarding Customer Information* (FTC 16 CFR Part 314) on May 23, 2002, with an effective date of May 23, 2003.

The Federal Trade Commission (FTC) Safeguards Act

As noted earlier, a wide variety of companies are subject to GLBA regulations. Banks, credit unions, insurance agencies, and investment firms are subject to regulatory oversight by the agency that charters or licenses them. The FTC has jurisdiction over individuals or organizations that are significantly engaged in providing financial products or services to consumers and are not subject to regulatory oversight. Many of these organizations are small businesses. The FTC's implementation is known as the ***Safeguards Act***. Overall, the requirements of the Safeguards Act are not as stringent as the Interagency Guidelines. The primary requirements are that covered entities must do the following:

- Designate the employee or employees to coordinate the safeguards
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks
- Design a safeguards program, and detail the plans to monitor it
- Select appropriate service providers and require them (by contract) to implement the safeguards
- Evaluate the program and explain adjustments in light of changes to its business arrangements or the results of its security tests

The FTC does not conduct regulatory compliance audits. Enforcement is complaint driven. Consumers can file a complaint with the FTC. The FTC analyzes the complaints and if it detects a pattern of wrongdoing, it will investigate and prosecute, if appropriate. The FTC does not resolve individual consumer complaints. Table 13.1 provides the GLBA regulatory agencies and their respective rules.

TABLE 13.1 GLBA Regulatory Agencies and Rules

Regulatory Agency	Institutions Type	GLBA Rule Federal Register Designation
Federal Reserve Board (FRB)	Bank holding companies and member banks of the Federal Reserve System (FRS)	12 C.F.R. § 216
Office of the Comptroller of the Currency (OCC)	National banks, federal savings associations, and federal branches of foreign banks	12 C.F.R. § 40
Federal Deposit Insurance Corporation (FDIC)	State-chartered banks (that are not members of the FRS)	12 C.F.R. § 332
National Credit Union Administration (NCUA)	Federally chartered credit unions	NCUA: 12 C.F.R. § 716
Securities and Exchange Commission (SEC)	Securities brokers and dealers as well as investment companies	17 C.F.R. § 248
Commodity Futures Trading Commission (CFTC)	Futures and option markets	CFTC: 17 C.F.R. § 160
Federal Trade Commission (FTC)	Institutions not covered by the other agencies	16 C.F.R. § 313

FYI: What Is the Federal Register?

Published by the Office of the Federal Register, National Archives and Records Administration (NARA), the Federal Register is the official daily publication for rules, proposed rules, and notices of federal agencies and organizations, as well as executive orders and other presidential documents. It is updated daily by 6 a.m. and is published Monday through Friday, except on federal holidays. The official home page of the Federal Register is www.federalregister.gov.

What Are the Interagency Guidelines?

As noted earlier, the financial services oversight agencies were tasked with independently establishing minimum-security standards as well as determining the type and severity of the penalties. Banks are subject to the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, and credit unions are subject to the Guidelines for Safeguarding Member Information. In this section, we will refer to them collectively as the *Interagency Guidelines*.

The ***Interagency Guidelines*** require every covered institution to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank or credit union and the nature and scope of its activities. To be in compliance, the information security program must include policies and processes that require institutions to do the following:

- Involve the Board of Directors
- Assess risk
- Manage and control risk
- Oversee service provider arrangements
- Adjust the program
- Report to the Board

It is up to each institution to develop a program that meets these objectives. The ISO 27002:2013 standard provides an excellent framework to develop a GLBA-compliant information security program.

In Practice

Regulatory Language Definitions

To understand the scope and mandate of the information security regulations, we need to start with the terminology. The following definitions apply to all versions of the Interagency Guidelines. Note that with the exception of credit unions, the user of services is referred to as a *customer* (in the case of credit unions, they are referred to as *members*).

- ***Consumer information*** means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on behalf of the institution for a business purpose. The term does not include any record that does not personally identify an individual.
- ***Customer or member information*** means any record containing NPPI, about a customer or member, whether in paper, electronic, or other form, that is maintained by or on behalf of the financial institution.
- ***Customer or member information system*** means any method used to access, collect, store, use, transmit, protect, or dispose of customer or member information.
- ***Service provider*** means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the financial institution.
- ***Administrative safeguards*** are defined as governance, risk management, oversight, policies, standards, processes, programs, monitoring, and training designed and implemented with the intent of establishing and maintaining a secure environment.
- ***Technical safeguards*** are defined as controls that are implemented or enforced by technological means.
- ***Physical safeguards*** are defined as controls designed to protect systems and physical facilities from natural threats and/or man-made intrusions.

Involve the Board of Directors

The Interagency Guidelines require that the Board of Directors or an appropriate committee of the Board approve the bank's written information security program. The Board is also tasked with overseeing the development, implementation, and maintenance of the information security program, including assigning specific responsibility for its implementation and reviewing reports from management. As corporate officials, directors have a fiduciary and legal responsibility. For example, financial institutions that do not comply with the GLBA are subject to civil penalties of $100,000 *per violation.* Officers and directors of that institution can be held personally liable as well, with penalties of $10,000 *per violation.*

Board members are generally chosen for their experience, business acumen, and standing in the community. It can be assumed that they understand business goals, processes, and inherent risks. Even experienced professionals, however, do not always have an in-depth natural understanding of information security issues. Institutions are expected to provide their Boards with educational opportunities to become and remain proficient in the area. Recognizing that this is a specialized body of knowledge, the Interagency Guidelines include the provision for delegation and distribution of responsibilities.

Examples of delegation include the following:

- Delegating Board oversight to a subcommittee whose members include directors and representatives of the financial institution, such as a Chief Information Security Officer (CISO) or Chief Risk Officer (CRO)

- Assigning information security management program oversight and management to a CISO or CRO
- Assigning implementation and maintenance of administrative controls to the Information Security Officer
- Assigning implementation and maintenance of technical controls to the Director of Information Technology
- Assigning implementation and maintenance of physical controls to the facilities manager
- Assigning design and delivery of information security training and awareness programs to the training department
- Assigning verification of controls to the internal audit department
- Assigning risk evaluation to the risk management committee
- Assigning the evaluation of technology initiatives to the technology steering committee
- Creating a multidisciplinary information security advisory committee that includes the representatives of all of the aforementioned roles and departments

Information security crosses many boundaries and involves multiple domains. Experience has shown us that institutions that have adopted a cross-functional multidisciplinary approach, as shown in Figure 13.1, have a stronger and more successful information security program.

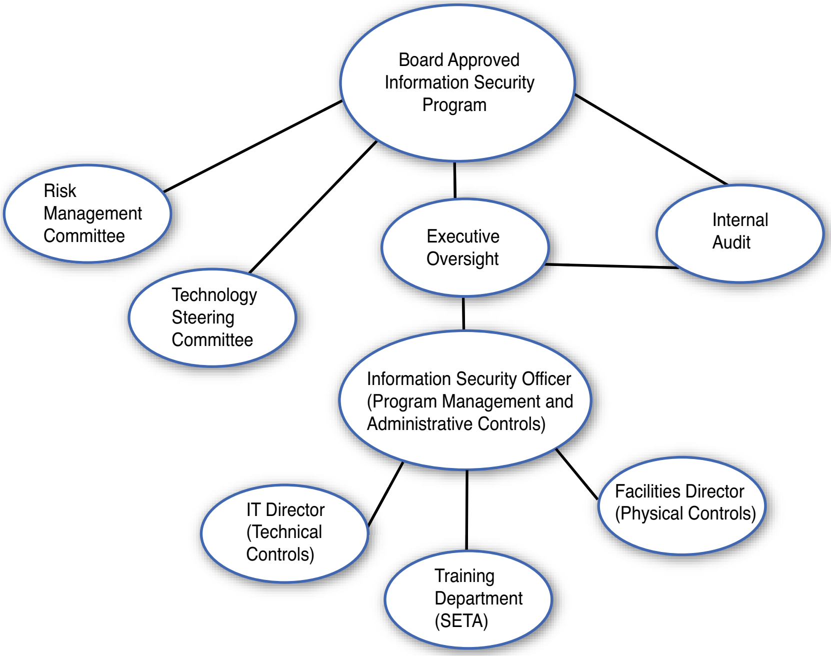

Board Approved Information Security Program
Risk Management Committee
Technology Steering Committee
Executive Oversight
Internal Audit
Information Security Officer (Program Management and Administrative Controls)
IT Director (Technical Controls)
Training Department (SETA)
Facilities Director (Physical Controls)

FIGURE 13.1 A cross-functional multi-disciplinary approach.

In Practice

GLBA Section III-A: Involve the Board of Directors

The Board of Directors or an appropriate committee of the Board of each bank or credit union shall:

- Approve the written information security program
- Oversee the development, implementation, and maintenance of the information security program, including assigning specific responsibility for its implementation and reviewing reports from management

Assess Risk

Financial institutions are expected to take a risk-based approach to information security. The process begins with identifying threats. ***Threats*** are defined as potential dangers that have the capacity to cause harm. It is incumbent upon each institution to continually engage in a ***threat assessment***, which is the identification of the types of threats and attacks that may affect the institution's condition and operations or may cause data disclosures that could result in substantial harm or inconvenience to customers. A threat assessment must take into consideration a number of factors, including the size and type of the institution, services offered, geographic location, experience of personnel, infrastructure design, operating systems, vulnerability of applications, and cultural attitudes and norms. At a minimum, financial institutions must address the threats of unauthorized access, unauthorized data modification, system infiltration, malware, destruction of data or systems, and denial of service (DoS).

The systematic rating of threats based on level of impact and likelihood sans controls is used to determine the ***inherent risk***. A ***risk assessment*** is used to evaluate the corresponding safeguards in order to calculate ***residual risk***, which is defined as the level of risk after controls have been implemented. The Federal Financial Institutions Examination Council (FFIEC) recommends using the NIST risk management framework and methodology as described in Special Publication 800-53 to calculate residual risk. Multiple categories of risk are defined by the FDIC as relevant for financial institutions, including strategic, reputational, operational, transactional, and compliance:

- ***Strategic risk*** is the risk arising from adverse business decisions, or the failure to implement appropriate business decisions in a manner that is consistent with the institution's strategic goals.
- ***Reputational risk*** is the risk arising from negative public opinion.
- ***Operational risk*** is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.
- ***Transactional risk*** is the risk arising from problems with service or product delivery.
- ***Compliance risk*** is the risk arising from violations of laws, rules, or regulations, or from noncompliance with internal policies or procedures or with the institution's business standards.

Risk assessments and corresponding risk management decisions must be documented and reported to the Board of Directors or designee. The reports are used by both independent auditors and regulators to evaluate the sufficiency of the institution's risk management program.

In Practice

GLBA Section III-B: Assess Risk

Each bank or credit union shall:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
- Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

Manage and Control Risk

The Interagency Guidelines require that financial institutions design their information security programs to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of their activities. The agencies recommend using the ISO standards as the framework for financial institution information security programs. Table 13.2 maps the GLBA information security objectives and the ISO security domains.

TABLE 13.2 GLBA Requirement ISO 27002:2013 Cross Reference

GLBA Requirement	Corresponding ISO 27002:2013 Domain
II. Standards for Safeguarding Customer Information	
A. Information Security Program Requirements	Information Security Policies Compliance Management
III. Development and Implementation of Information Security Program	
A. Involve the Board of Directors	Organization of Information Security
B. Assess Risk	Refer to ISO 27005: Risk Management

GLBA Requirement	Corresponding ISO 27002:2013 Domain
C1. Manage and Control Risk	Asset Management Human Resources Security Physical and Environmental Security Communications Security Operations Security Access Control Information Systems Acquisition, Development, and Maintenance Information Security Incident Management Business Continuity
C2. Train Staff	Human Resources Security
C3. Test Key Controls	Communications Security Operations Security Information Systems Acquisition, Development, and Maintenance Information Security Incident Management Business Continuity
C4. Properly Dispose of Information	Asset Management
D. Oversee Service Provider Arrangements	Communications Security Operations Security
E. Adjust the Program	Information Security Policies Compliance Management
F. Report to the Board	Organization of Information Security
Supplement A to Appendix B to Part 364 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice	Information Security Incident Management

A must-read supporting resource is IT InfoBase published by the Federal Financial Institutions Examination Council (FFIEC). The FFIEC is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the FDIC, the NCUA, the OCC, and the OTS, and to make recommendations to promote uniformity in the supervision of financial institutions. The IT InfoBase spans a number of topics, including Information Security, IT Audit, Business Continuity Planning, Development and Acquisition, Management, Operations, and Outsourcing Technology Services.

The FFIEC InfoBase is the de facto guide for a financial institution that wants to ensure it has a GLBA-compliant information security program that meets regulatory expectations. Resources include explanatory text, guidance, recommended examination procedures and work papers, presentations, and resource pointers. The InfoBase can be accessed from the FFIEC home page (www.ffiec.gov).

In Practice

GLBA Section IIIC-1: Manage and Control Risk

Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may fraudulently seek to obtain this information.
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities, to permit access only to authorized individuals.
- Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access.
- Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program.
- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information.
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.
- Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.
- Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

Training

The Interagency Guidelines require institutions to implement an ongoing information security awareness program, to invest in training, and to educate executive management and directors. This is widely interpreted as embodying the NIST SETA model of security education, training, and awareness (SETA). You may recall this model from Chapter 6, "Human Resources Security." The goal of education is to explain why, and the anticipated outcome is insight and understanding. The goal of training is to explain how, and the anticipated outcome is knowledge and skill. Lastly, the goal of awareness is to explain what, and the anticipated outcome is information and awareness. The impact of education is long term, the impact of training is immediate, and the impact of awareness is short term.

At a minimum, financial institutions are expected to deliver and document annual enterprise-wide training. The training can be instructor led or online. Recommended topics include an overview of state and federal regulatory requirements, an explanation of user-focused threats such as malware and social engineering, and a discussion of best practices and information resources acceptable use. It is commonplace for institutions to coordinate the distribution and signing on the acceptable use agreement with the annual training.

In Practice

GLBA Section IIIC-2: Training

Train staff to implement the bank's information security program.

Testing

Safeguards are meaningful only if they perform as anticipated. The regulatory agencies expect institutions to regularly test key controls and safeguards at a frequency that takes into account the rapid evolution of threats. High-risk systems should be subject to independent testing at least once a year. Independent testing means that the in-house or outsourced personnel who perform and report on the testing have no relationship to the design, installation, maintenance, and operation of the targeted system, or the policies and procedures that guide its operation. They should also be protected from undue influence or retaliatory repercussions.

The tests and methods utilized should be sufficient to validate the effectiveness of the security process in identifying and appropriately controlling security risks. The three most commonly used testing methodologies are audit, assessment, and assurance:

- An ***audit*** is an evidence-based examination that compares current practices against a specific internal (for example, policy) or external (for example, regulations or audit standard such as Control Objectives for Information and Related Technology [COBIT]) criteria.
- An ***assessment*** is a focused privileged inspection to determine condition, locate weakness or vulnerabilities, and identify corrective actions.
- An ***assurance*** test measures how well the control or safeguard works generally by subjecting the system or device to an actual attack, misuse, or an accident. Assurance tests can be ***black box***, meaning with no prior knowledge of the system or process being tested, or ***white box***, meaning with knowledge of the system or process being tested.

Because testing may uncover non-public customer information, appropriate safeguards to protect the information must be in place. Contracts with third parties that provide testing services should require that the third parties implement appropriate measures to meet the objectives of the Interagency Guidelines and that any exposure of NPPI be reported immediately.

In Practice

GLBA Section IIIC-3: Testing

Regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

Oversee Service Provider Arrangements

A ***third-party service provider relationship*** is broadly defined by the regulatory agencies to include all entities that have entered into a business relationship with a financial institution. This includes parties that perform functions on behalf of the institution, provide access to products and services, or perform marketing, monitoring, or auditing functions.

The Interagency Guidelines require financial institutions to ensure that service providers have implemented security controls in accordance with GLBA requirements. In June 2008, the Financial Institution Letter FIL-44-2008 "Third-Party Risk Guidance for Managing Third-Party Risk" made clear that an "institution can outsource a task, but it cannot outsource the responsibility." It is up to the institution to ensure that the controls and safeguards designed, managed, and maintained by third parties are equivalent to or exceed internal policies and standards.

Recommended service provider oversight procedures include the following:

- Conducting a risk assessment to ensure that the relationship is consistent with the overall business strategy and to ensure that management has the knowledge and expertise to provide adequate oversight
- Using appropriate due diligence in service provider research and selection
- Implementing contractual assurances regarding security responsibilities, controls, and reporting
- Requiring non-disclosure agreements (NDAs) regarding the institution's systems and data
- Providing a third-party review of the service provider's security though appropriate audits and tests
- Coordinating incident response policies and contractual notification requirements
- Reviewing at least annually significant third-party arrangements and performance

The ***Bank Service Company Act (BSCA)***, 12 USC 1861-1867, gives federal financial regulators statutory authority to regulate and examine the services a technology service provider (TSP) performs for FDIC-insured financial institutions. According to the FFIEC Outsourcing Technology Services Handbook, TSP relationships should be subject to the same risk management, security, privacy, and other internal controls and policies that would be expected if the financial institution were conducting the activities directly. In order to maintain an accurate database of TSPs, BSCA requires insured financial institutions to notify their appropriate federal banking agency in writing of contracts or relationships with third parties that provide certain services to the institution. Selected TSPs are examined on a 24-, 36-, or 48-month cycle. Distribution of the exam results is restricted to financial institutions that have signed a contract with the TSP. Ironically, this means that the findings are not available during the initial due-diligence phase.

In Practice

GLBA Section III-D: Oversee Service Provider Relationships

Each bank shall:

- Exercise appropriate due diligence in selecting its service providers.
- Require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines.
- Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

Adjust the Program

A static information security program provides a false sense of security. Threats are ever increasing. Organizations are subject to change. Monitoring the effectiveness of the security program and personnel is essential to maintaining a secure environment, protecting customer information, and complying with regulatory objectives. Evaluation results should be carefully analyzed and, as appropriate, adjustments to the information security program implemented. At a minimum, the information security policy should be reviewed annually. Modifications to policy must be communicated to the Board of Directors. It is the responsibility of the Board of Directors to annually reauthorize the information security policy and, by extension, the information security program.

In Practice

GLBA Section III-E: Adjust the Program

Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

Report to the Board

Throughout the year, the Board of Directors or designated committee should receive information security program updates and be immediately apprised of any major issue. Additionally, the Interagency Guidelines require each institution to provide an annual Information Security and GLBA Compliance report to the Board of Directors or designated committee. The report should describe the overall status of the information security program and the bank's compliance with the Interagency Guidelines. The report should detail the following:

- Regulatory examination results and post-examination follow-up.
- Security incidents that occurred in the previous 12 months, including a synopsis of response and impact.
- Major IT and security initiatives completed in the previous 12 months, in progress and scheduled.
- Information security program–related governance activities, including a synopsis of roles, responsibilities, and significant decisions.
- Independent audit and testing conducted in the previous 12 months. The description should include type of test, date of test, tester, test objective, test results, recommendations, follow-up, and, if applicable, remediation plan.
- Risk assessments conducted in the previous 12 months. The description should include methodology, focus areas, results, follow-up, and, if applicable, remediation plan.
- Service provider oversight activities. The description should include due diligence, contract updates, monitoring, and, if applicable, identified issues and remediation plan.
- Employee training conducted in the previous 12 months. The description should include the type of training, conduct, participation, and evaluation.
- Updates to and testing of the incident disaster recovery, public health emergency, and business continuity plan.
- Updates to and testing of the incident response plan and procedures.
- Recommended changes to the information security program or policy that require Board approval or authorization.

The final section of the report should be management's opinion of the institution's compliance with information security–related state and federal regulations and guidance. Conversely, if in management's opinion the institution does not comply with applicable regulations or guidance, the issues should be fully documented and a remediation plan presented.

What Is a Regulatory Examination?

The regulatory agencies are responsible for oversight and supervision of financial institutions. Included in this charge is ensuring the financial institutions soundly manage risk, comply with laws and regulations, including GLBA, and, as appropriate, take corrective action. Representatives of the regulatory agencies examine their respective banks and credits unions. Depending on size, scope, and previous examination findings, exams are conducted every 12 to 18 months. Included in the exam is an evaluation of policies, processes, personnel, controls, and outcomes.

Examination Process

GLBA security is included in the Information Technology Examination. Institutions are given 30 to 90 days notice that an examination is scheduled. An Information Technology Officer's questionnaire is sent to the institution with the expectation that the institution will complete and return the questionnaire and supporting documentation (including Board reports, policies, risk assessments, test results, and training materials) prior to the examination date. The length of the exam and number of on-site examiners depends on the complexity of the environment, previous findings, and examiner availability. The examination begins with an entrance meeting with management. The agenda of the entrance meeting includes explaining the scope of the examination, the role of each examiner, and how the team will conduct the exam. During the exam, the examiners will request information, observe, and ask questions. At the end of the exam, an exit meeting is held to discuss findings and potential solutions. Post-examination, the regulatory agency will issue a draft report for management's review for accuracy. Taking into consideration management's response, the agency will issue a written report to the Board of Directors, which includes the examination ratings, any issues that have been identified, recommendations, and, if required, supervisory action.

Examination Ratings

The ***Uniform Rating System for Information Technology (URSIT***) is used to uniformly assess financial institutions. The rating is based on a scale of 1 to 5, in ascending order of supervisory concern, with 1 representing the best rating and least degree of concern, and 5 representing the worst rating and highest degree of concern.

Per URSIT standards:

- Financial institutions that are rated as a "1" exhibit strong performance in every respect. Weaknesses in IT are minor in nature and are easily corrected during the normal course of business. Risk management processes provide a comprehensive program to identify and monitor risk relative to the size, complexity, and risk profile of the entity.
- Financial institutions rated as a "2" exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes, or system development. Generally, senior management corrects weaknesses in the normal course of business. Risk management processes adequately identify and monitor risk relative to the size, complexity, and risk profile of the entity. As a result, supervisory action is informal and limited.

- Financial institutions and service providers rated composite "3" exhibit some degree of supervisory concern because of a combination of weaknesses that may range from moderate to severe. If weaknesses persist, further deterioration in the condition and performance of the institution or service provider is likely. Risk management processes may not effectively identify risks and may not be appropriate for the size, complexity, or risk profile of the entity. Formal or informal supervisory action may be necessary to secure corrective action.
- Financial institutions and service providers rated composite "4" operate in an unsafe and unsound environment that may impair the future viability of the entity. Operating weaknesses are indicative of serious managerial deficiencies. Risk management processes inadequately identify and monitor risk, and practices are not appropriate given the size, complexity, and risk profile of the entity. Close supervisory attention is necessary and, in most cases, formal enforcement action is warranted.
- Financial institutions and service providers rated composite "5" exhibit critically deficient operating performance and are in need of immediate remedial action. Operational problems and serious weaknesses may exist throughout the organization. Risk management processes are severely deficient and provide management little or no perception of risk relative to the size, complexity, and risk profile of the entity. Ongoing supervisory attention is necessary.

Supplemental to the rating, if violations of any law or regulations are identified, the agency must provide detailed information, including legal numerical citations and name, a brief description of the law or regulation (or portion of it) that is in violation, a description of what led to the violation, and corrective action taken or promised by management.

Personal and Corporate Identity Theft

Personal and corporate identity theft is one of the fastest growing crimes worldwide. ***Personal identity theft*** occurs when a criminal fraudulently uses a name, address, SSN, bank account or credit card account number, or other identifying information without consent to commit a crime. As reported by Javelin Strategy & Research in its "2013 Identity Fraud Report," 12.6 million U.S. adults were victims of identity theft. That figure represents 5.26% of U.S. adults.

- The top five states with the most ID theft complaints are, in order, Florida, California, Texas, New York, and Georgia.
- The total estimated cost of identity theft in 2012 was $21 billion, with an average per-incident loss of $4,930.
- The average victim spent $365 and 12 hours to resolve the problem and clear up records.

In response to this problem, in early 2005, the regulatory agencies issued Supplement A, "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice."

Corporate identity theft occurs when criminals attempt to impersonate authorized employees, generally for the purpose of accessing corporate bank accounts in order to steal money. This type of attack is known as a *corporate account takeover.* Using specially crafted malware, criminals capture a business's online banking credentials or compromise the workstation used for online banking. The criminals then access online accounts and create fraudulent ACH or wire transfers. The transfers are directed "money mules" who are waiting to withdraw the funds and send the money overseas. Once the funds are offshore, it is very difficult for law enforcement to recover them.

As many of these crimes go unreported, there are few definitive statistics regarding corporate account takeover activity. In early 2010, the U.S. FDIC estimated US$120 million in activity from online banking fraud involving the electronic transfer of funds in the third quarter of 2009. According to the most recent Account Takeover Survey from FS-ISAC's Account Takeover Task Force, financial institutions reported 87 account takeover attempts in 2009, 239 in 2010, and 314 annualized in 2011. According to the same survey, in 2011, 12 percent of account takeover attempts resulted in money leaving the banks, whereas in 2009, 70 percent of attacks involved money leaving the bank. In response to this problem, in October 2011, the regulatory agencies issued the Supplement to the Authentication in an Internet Banking Environment Guidance.

What Is Required by the Interagency Guidelines Supplement A?

Supplement A, "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," describes response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The guidance enumerates a number of security measures that each financial institution must consider and adopt, if appropriate, to control risks stemming from reasonably foreseeable internal and external threats to the institution's customer information. The guidance stresses that every financial institution must develop and implement a risk-based response program to address incidents of unauthorized access to customer information. The response program should be a key part of an institution's information security program. Supplement A emphasizes that an institution's response program should contain procedures for the following:

- Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused.
- Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information.
- Being consistent with the agencies' Suspicious Activity Report (SAR) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing.

- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information—for example, by monitoring, freezing, or closing affected accounts—while preserving records and other evidence.
- Requiring its service providers by contract to implement appropriate measures designed to protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customers.
- Notifying customers when warranted.

The guidance empathizes notification requirements. When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution is required to conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it must notify its regulatory agency and affected customers as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. In this case, the institution should notify its customers as soon as notification will no longer interfere with the investigation. When customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so.

Compliance with the Supplement A, "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," is included in the Information Technology Examination.

Identity Theft Data Clearinghouse

Although the FTC does not have criminal jurisdiction, it supports the identity theft criminal investigation and prosecution through its ***Identity Theft Data Clearinghouse***. The Clearinghouse is the nation's official repository for identity theft complaints and a part of the FTC's Consumer Sentinel complaint database. In addition to housing over a million ID theft complaints, Sentinel offers participating law enforcement agencies a variety of tools to facilitate the investigations and prosecution of identity theft. These include information to help agencies coordinate effective joint action, sample indictments, tools to refresh investigative data through programmed data searches, and access to "hot address" databases.

What Is Required by the Supplement to the Authentication in an Internet Banking Environment Guidance?

In response to the alarming rate of successful corporate account takeover attacks, the financial losses being sustained by both financial institutions and customers, and the impact on public confidence in the online banking system, in October 2011, the regulatory agencies issued updated guidance related to Internet banking safeguards. The Supplement to the Authentication in an Internet Banking Environment Guidance stressed the need for performing risk assessments, implementing effective strategies for mitigating identified risks, and raising customer awareness of potential risks. In a departure from other guidance, the supplement was specific in its requirements and opinion of various authentication mechanisms.

Requirements include the following:

- Financial institutions are required to review and update their existing *risk assessments* as new information becomes available, prior to implementing new electronic financial services, or at least every 12 months.
- Financial institutions are required to implement a layered security model. *Layered security* is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control.
- Financial institutions are required to offer *multifactor authentication* to their commercial cash management (ACH and wire transfer) customers. Because the frequency and dollar amounts of these transactions are generally higher than consumer transactions, they pose a comparatively increased level of risk to the institution and its customer.
- Financial institutions are required to implement authentication and transactional *fraud monitoring*.
- Financial institutions are required to educate their retail and commercial account holders about the risks associated with online banking. Commercial customers must be notified that their funds are not covered under Regulation E and that they may incur a loss. It is strongly recommended that the awareness programs include risk reduction and mitigation recommendations.

Compliance with the Supplement to the Authentication in an Internet Banking Environment Guidance has been added to the Information Technology Examination. Anecdotal evidence suggests that the guidance has had an impact as losses associated with corporate account takeover are declining.

FYI: Corporate Account Takeover Fraud Advisory

The United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), and the Financial Services Information Sharing and Analysis Center (FSISAC) jointly issued a Fraud Advisory for Business: Corporate Account Takeover, with the intent of warning business about this type of crime. The advisory noted that cybercriminals are targeting nonprofits, small and medium-sized businesses, municipalities, and school districts across the country. Using malicious software (malware), cybercriminals attempt to capture a business's online banking credentials, take over web sessions, or even remotely control the workstation. If the criminal gains access to online bank account login credentials or can take over an online banking session, it is possible for him to initiate and authorize ACH or wire funds transfers. Generally, the criminal will create numerous smaller transactions and send them to domestic "money mules," who are waiting to withdraw the funds and send the money overseas. Once the funds are offshore, it is very difficult for law enforcement to recover them. To make matters worse, financial institutions are not required to reimburse for fraud-related losses associated with commercial accountholder computers or networks. Nor are these losses covered by FDIC insurance.

The information contained in the advisory is intended to provide basic guidance and resources for businesses to learn about the evolving threats and to establish security processes specific to their needs. The advisory as well as related resources are available at the NACHA Corporate Account Takeover Resource Center website at www.nacha.org/Corporate_Account_Takeover_Resource_Center. Security journalist Brian Krebs has been reporting on the impact of corporate account takeovers on small business since 2009. For current and archived reports, visit his blog at http://krebsonsecurity.com/category/smallbizvictims.

Summary

Federal law defines a financial institution as “any institution the business of which is significantly engaged in financial activities….” This broad definition includes banks, credit unions, investment firms, and businesses such as automobile dealers, check-cashing businesses, consumer reporting agencies, credit card companies, educational institutions that provide financial aid, financial planners, insurance companies, mortgage brokers and lenders, and retail stores that issue credit cards.

In 1999, Congress enacted legislation requiring all financial institutions that do business in the United States to protect the privacy and security of customer non-public personal information (NPPI). The Gramm-Leach-Bliley Act (GLBA) required that appropriate privacy and security standards be developed and enforced, and assigned this task to various federal agencies. The agencies that regulate banks and credit unions collaborated and in 2001 published the Interagency Guidelines Establishing Standards for Safeguarding Customer Information and the Guidelines for Safeguarding Member Information, respectively. The Federal Trade Commission (FTC) was charged with developing standards for nonregulated businesses that provide financial services, and in 2003 published the Standards for Safeguarding Customer Information, also known as the Safeguards Act. Due to the type of business the regulations apply to, the requirements of the Safeguards Act are not as stringent as the Interagency Guidelines. The FTC does not conduct compliance examinations. The basis for investigation and enforcement actions are consumer complaints.

The Interagency Guidelines Establishing Standards for Safeguarding Customer Information and the Guidelines for Safeguarding Member Information, collectively referred to as the Interagency Guidelines, define information security program objectives and requirements for banks and credit unions. It is up to each covered entity to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. To be in compliance, the information security program must include policies and processes that require institutions to do the following:

- Involve the Board of Directors
- Assess risk
- Manage and control risk
- Oversee service provider arrangements
- Adjust the program
- Report to the Board

It is up to each institution to develop a program that meets these objectives. The ISO 27002:2013 standard provides an excellent framework for a GLBA-compliant information security program.

Financial institutions are expected to take a risk-based approach to information security. The process begins with identifying threats. Threats are defined as potential dangers that have the capacity to cause harm. It is incumbent upon each institution to continually engage in a threat assessment. A threat assessment is the identification of the types of threats and attacks that may affect the institution's condition and operations or may cause data disclosures that could result in substantial harm or inconvenience to customers. At a minimum, financial institutions must address the threats of unauthorized access, unauthorized data modification, system infiltration, malware, destruction of data or systems, and DoS. The systematic rating of threats based on level of impact and likelihood sans controls is used to determine the inherent risk. A risk assessment is used to evaluate the corresponding safeguards in order to calculate residual risk. Residual risk is defined as the level of risk after controls and safeguards have been implemented. The FFIEC recommends using the NIST risk management framework and methodology as described in Special Publication 800-53 to calculate residual risk. Multiple categories of risk are defined by the FDIC as relevant for financial institutions, including strategic, reputational, operational, transactional, and compliance.

Controls and safeguards can be circumvented by users. Although these actions may be deliberate or accidental, they are often intentionally malicious. In order to mitigate the risk of circumvention, it is critical that users understand the threat environment, learn best practices, and agree to acceptable use of information and information systems. To this end, institutions are expected to have a security awareness program and to provide annual enterprise-wide training.

Controls and safeguards are only useful if they perform as expected. Scheduled testing should be conducted by personnel that are independent of the targeted system. The tests and methods utilized should be sufficient to validate the effectiveness of the controls and safeguards. The three most common testing methodologies are audit, assessment, and assurance.

The Interagency Guidelines require financial institutions to ensure that service providers have implemented security controls in accordance with GLBA requirements. Financial Institution Letter FIL-44-2008, "Third-Party Risk Guidance for Managing Third-Party Risk," clearly states that an institution can outsource a task, but it cannot outsource the responsibility. It is up to the institution to ensure that the controls and safeguards designed, managed, and maintained by third parties comply with the Interagency Guidelines and are equivalent to or exceed internal policies and standards.

The financial institutions' Board of Directors is ultimately responsible for oversight of the information security program and for compliance with all applicable state and federal regulations. Throughout the year, board members should receive information security program updates and be immediately apprised of all major security issues. Decisions that may significantly affect the risk profile of the institution must be authorized by the Board. The Interagency Guidelines require each institution to provide a comprehensive annual Information Security and GLBA Compliance report to the Board of Directors or designated committee.

In response to the problem of personal and corporate identity threat, in 2005 the regulatory agencies issued Supplement A, "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice," and in 2011, Supplement to the Authentication in an

Internet Banking Environment Guidance. Both supplements focus on threats related to unauthorized access to or use of customer information as well as corresponding controls, including education, incident response programs, and notification procedures.

To ensure compliance with GLBA Interagency Guidelines and supplemental guidance, financial institutions are subject to regulatory examinations. Depending on size, scope, and previous examination findings, exams are conducted every 12 to 18 months. Included in the exam is an evaluation of policies, processes, personnel, controls, and outcomes. The outcome of the examination is a rating based on a scale of 1 to 5, in ascending order of supervisory concern (1 representing the best rating and least degree of concern, and 5 representing the worst rating and highest degree of concern), supervisory comments, and recommendations. Financial institutions that are found not in compliance with regulatory requirements and do not remediate examination findings within an agreed-upon timeframe can be subject to closure.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following statements best defines the type of organizations that are subject to GLBA regulations?

   A. GLBA applies only to banks and credit unions.

   B. GLBA applies only to check cashing businesses.

   C. GLBA applies to any business engaged in financial services.

   D. GLBA applies only to institutions licensed to offer depository services.

2. The Financial Modernization Act of 1999 __________________.

   A. deregulated financial services

   B. mandated use of computers

   C. required banks and credit unions to merge

   D. prohibited banks from controlling a nonbanking company

3. The GLBA requires financial institutions to protect which of the following?

   A. The privacy of customer NPPI

   B. The security of customer NPPI

   C. The privacy and the security of customer NPPI

   D. None of the above

4. Which of the following is *not* considered NPPI?

   A. SSN

   B. Name

   C. Checking account number

   D. PIN or password associated with a financial account or payment card

5. The Interagency Guidelines Establishing Standards for Safeguarding Customer Information was jointly developed by the ____________________________.

   A. Federal Deposit Insurance Corporation (FDIC)

   B. Office of the Comptroller of the Currency (OCC), Federal Reserve System (FRS), FDIC, and Office of Thrift Supervision (OTS)

   C. Securities and Exchange Commission (SEC) and FDIC

   D. National Credit Union Administration (NCUA) and FDIC

6. Which of the following entities developed, published, and enforced the Safeguards Act?

   A. Federal Reserve System (FRS)

   B. Securities and Exchange Commission (SEC)

   C. Federal Trade Commission (FTC)

   D. Federal Deposit Insurance Corporation (FDIC)

7. Which of the following statements is false?

   A. The Safeguards Act applies to all federally insured institutions.

   B. Compliance with the Safeguards Act is not proactively audited.

   C. The Interagency Guidelines are more stringent than the Safeguards Act.

   D. Enforcement of the Safeguards Act begins with a complaint.

8. The Interagency Guidelines require a written security program that includes all of the following except ____________.

   A. legal safeguards

   B. physical safeguards

   C. technical safeguards

   D. administrative safeguards

9. Financial institutions can be fined up to _____ per violation.

   A. $100

   B. $1,000

   C. $10,000

   D. $100,000

10. Financial institutions are expected to take a _________ approach to information security.

    A. threat-based
    B. risk-based
    C. audit-based
    D. management-based

11. Which of the following terms describes a potential danger that has the capacity to cause harm?

    A. Risk
    B. Threat
    C. Variable
    D. Vulnerability

12. Which of the following statements best describes a threat assessment?

    A. A threat assessment identifies the types of threats that may affect the institution or customers.
    B. A threat assessment is a systematic rating of threats based on level of impact and likelihood.
    C. A threat assessment is an audit report.
    D. A threat assessment is a determination of inherent risk.

13. Which of the following risk types is defined as a level of risk after controls and safeguards have been implemented?

    A. Ongoing risk
    B. Residual risk
    C. Acceptable risk
    D. Inherent risk

14. Which of the following risk management frameworks is recommended by the FFIEC?

    A. Basil
    B. COBIT
    C. NIST
    D. FDIC

15. Which of the following statements is true?

    A. Strategic risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

    B. Reputational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

    C. Transactional risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

    D. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.

16. The risk arising from problems with service or product delivery is known as ________________.

    A. strategic risk

    B. reputational risk

    C. transactional risk

    D. operational risk

17. At a minimum, financial institutions are expected to deliver user-focused information security training _________.

    A. quarterly

    B. semi-annually

    C. annually

    D. bi-annually

18. A security awareness and training program is considered which type of control?

    A. Administrative control

    B. Physical control

    C. Technical control

    D. Contractual control

19. Which of the following statements best describes independent testing?

    A. Independent testing is testing performed by a contractor.

    B. Independent testing is testing performed by personnel not associated with the target system.

    C. Independent testing is testing performed by personnel with security clearance.

    D. Independent testing is testing performed by certified professionals.

20. Which of the following test methodologies is a privileged inspection to determine condition, locate weakness or vulnerabilities, and identify corrective actions?

    A. Audit

    B. Assessment

    C. White box

    D. Black box

21. The statement, "An institution can outsource a task, but it cannot outsource the responsibility," applies to an organization's relationship with ________.

    A. regulators

    B. employees

    C. directors

    D. service providers

22. Per the Interagency Guidance, which of the following entities is responsible for oversight of a financial institution's Information Security Program?

    A. Chief Executive Officer (CEO)

    B. Information Security Officer

    C. Board of Directors

    D. Regulatory Agencies

23. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it must notify ____________.

    A. its regulatory agency

    B. affected customers

    C. Board of Directors

    D. All of the above

24. Which of the following statements is *not* true about financial institution regulatory examination?

    A. All institutions are subject to a three-year examination schedule.

    B. A rating scale of 1 to 5 is used to represent supervisory concern.

    C. Institutions found not in compliance can be subject to closure.

    D. Results are presented to the Board of Directors.

25. Which of the following statements best defines a corporate account takeover attack?

    A. Personal information is used to apply for a loan.

    B. Users are denied access to online banking.

    C. Fraudulent ACH and wire transfers are initiated from a commercial account.

    D. Corporate logos are used in phishing emails.

26. Which of the following is an example of multifactor authentication?

    A. Password and PIN

    B. Password and picture

    C. Password and challenge question

    D. Password and out-of-band code

27. Which of the following terms best describes the Supplemental Authentication Guidance requirement of layered defense?

    A. Dual control

    B. Separation of duties

    C. Defense in depth

    D. Need-to-know

28. Which of the following statements is true?

    A. When a financial institution chooses to outsource a banking function, it must conduct a due-diligence investigation.

    B. When a financial institution chooses to outsource a banking function, it must report the relationship to its regulatory agency.

    C. When a financial institution chooses to outsource a banking function, it must require the service provider to have appropriate controls and safeguards.

    D. All of the above.

29. Which of the following agencies is responsible for investigating consumer security–related complaints about a university financial aid office?

    A. FTC

    B. Department of Education

    C. FDIC

    D. Sallie Mae

30. Banks have customers; credit unions have ________.

    A. members

    B. supporters

    C. constituents

    D. incorporators

EXERCISES

EXERCISE 13.1: Identifying Regulatory Relationships

1. Access the official websites of the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC) and write a brief synopsis of the mission of each agency.
2. For each agency, identify at least one financial institution (within a 50-mile radius of your location) that it regulates.
3. In matters of information security, should it matter to consumers who regulates the financial institution they use? Why or why not?

EXERCISE 13.2: Researching the FTC

1. Visit the official FTC website and write a brief synopsis of its mission.
2. Prepare a summary of FTC information security resources for business.
3. Prepare a summary of an FTC GLBA-related enforcement action.

EXERCISE 13.3: Understanding the Federal Register

1. Locate a Federal Register copy of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.
2. Highlight the actual regulations.
3. Prepare a brief explaining the other sections of the document.

EXERCISE 13.4: Assessing GLBA Training

1. Go online and find publicly available GLBA-related information security training.
2. Go through the training and make a list of the key points.
3. Did you find the training effective? Why or why not?

EXERCISE 13.5: Researching Identity Theft

1. Document the steps consumers should take if they have been or suspect they have been the victims of identity theft.
2. Document how a consumer reports identity theft to your local or state police.
3. Document how a consumer files an identity theft complaint with the FTC.

PROJECTS

PROJECT 13.1: Educational Institutions and GLBA

Educational institutions that collect, process, store, and/or transmit non-public personal student information, including financial records and SSNs, are subject to GLBA regulations.

1. Locate documents published by your school that relate to compliance with GLBA. If you are not a student, choose a local educational institution. GLBA compliance documentation is generally published on an institution's website.
2. Evaluate the documentation for clarity (for example, is it written in plain language? is it easy to understand and relate to?) and content (does it address the objectives of the Safeguards Act?). Make suggestions for improvement.
3. Prepare a training session for new faculty and administration that describes the school's GLBA compliance policy and standards. Include an explanation of why it is important to safeguard NPPI.

PROJECT 13.2: Understanding Third-Party Oversight

GLBA Section III-D requires financial institutions to "oversee service provider relationships."

1. Explain what is meant by the phrase "an institution can outsource a task, but it cannot outsource the responsibility."
2. Access a copy of Financial Institution Letter FIL-44-2008, "Third-Party Risk Guidance for Managing Third-Party Risk." What actions should an institution take to ensure the service provider is in compliance with regulatory requirements?
3. In October 2012, the FFIEC published an updated Supervision of Technology Service Providers InfoBase. Access the handbook and read the sections titled "Report of Examination," "ROE Distribution," and "Customer List." A bad report can seriously harm a service provider. Prepare a brief for or against the examination of service providers and the distribution of the report.

PROJECT 13.3: Assessing Risk Management

According to the FFIEC Information Security InfoBase Handbook (Appendix A), the initial step in a regulatory Information Technology Examination is to interview management and review examination information to identify changes to the technology infrastructure, new products and services, or organizational structure.

1. Explain how changes in network topology, system configuration, or business processes might increase the institution's information security–related risk. Provide examples.
2. Explain how new products or services delivered to either internal or external users might increase the institution's information security–related risk. Provide examples.
3. Explain how loss or addition of key personnel, key management changes, or internal reorganizations might increase the institution's information security–related risk. Provide examples.

Case Study

Corporate Account Takeover Attack

Corporate account takeover attacks have cost small businesses, municipalities, and nonprofits hundreds of thousands of dollars. PATCO, a family-owned construction firm, was the victim of a 2009 corporate account takeover. Over a ten-day period, the criminals successfully transferred $588,000 from PATCO's account at Ocean National Bank to money mules throughout the country.

1. The criminals used Zeus malware to steal the login credentials. Research Zeus and write a brief describing the origin of the malware, how it is delivered to potential victims, what it is capable of, and what controls can be put in place to mitigate its effect.
2. PATCO sued Ocean National Bank to recover the lost funds. Research the case and write a synopsis of the Appeals Court July 2, 2012 ruling.
3. What requirement(s) of the 2011 Supplement to the Authentication in an Internet Banking Environment Guidance would have potentially prevented the attack from being successful?

References

Regulations Cited

"12 U.S.C. Chapter 18: Bank Service Companies, Section 1867 Regulation and Examination of Bank Service Companies," accessed 08/2013, www.gpo.gov/fdsys/pkg/USCODE-2010-title12/html/USCODE-2010-title12-chap18-sec1867.htm.

"16 CFR Part 314 Standards for Safeguarding Customer Information: Final Rule," accessed 05/2013, www.ftc.gov/os/2002/05/67fr36585.pdf.

"Appendix B to Part 364: Interagency Guidelines Establishing Information Security Standards," accessed 08/2013, www.fdic.gov/regulations/laws/rules/2000-8660.html.

"Financial Institution Letter (FIL-49-99), Bank Service Company Act," accessed 08/2013, www.fdic.gov/news/news/financial/1999/fil9949.html.

"Financial Institution Letter (FIL-44-2008), Third-Party Risk Guidance for Managing Third-Party Risk," accessed 08/2013, www.fdic.gov/news/news/financial/2008/fil08044.html.

"Supplemental Guidance on Internet Banking Authentication, June 28, 2011," official website of the FFIEC, accessed 08/2013, www.ffiec.gov/press/pr062811.htm.

Other References

"Bank Supervision Process: Comptrollers Handbook September 2007 (updated May 17, 2012)," Comptroller of the Currency, accessed 08/2013, www.occ.gov/publications/publications-by-type/comptrollers-handbook/banksupervisionprocess.html.

Chilingerian, Natasha. "FS-ISAC Survey Shows Uptick in Account Takeover Attempts, Drop in Actual Losses," *Credit Union Times*, June 15, 2012, accessed 08/2013, www.cutimes.com/2012/06/15/fs-isac-survey-shows-uptick-in-account-takeover-at.

"Consumer Information—Identity Theft," official website of the Federal Trade Commission, accessed 08/2013, www.consumer.ftc.gov/features/feature-0014-identity-theft.

"FDIC Oversight of Technology Service Providers, July 2006, Report No. 06-015," Audit Report, OIG Office of Audits, accessed 08/2013, www.fdicoig.gov/reports06/06-015-508.shtml.

"FFIEC Information Security IT Examination Handbook," July 2006, Federal Financial Institutions Examination Council, accessed 08/2013, http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

"FFIEC Supervision of Technology Service Providers (TSP) Handbook," October 2012, Federal Financial Institutions Examination Council, accessed 08/2013, http://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers-(tsp).aspx.

Field, Tom. "The FDIC on Vendor management—Interview with Donald Saxinger," Bank InfoSecurity, Sept. 27, 2010, accessed 08/2013, www.bankinfosecurity.com/interviews.php?interviewID=746.

"Fraud Advisory for Business: Corporate Account Takeover," U.S. Secret Service, FBI, IC3, and FS-ISAC, accessed 08/2013, www.nacha.org/Corporate_Account_Takeover_Resource_Center.

"FTC Resources for Reporters," official website of the Federal Trade Commission, accessed 08/2013, www.ftc.gov/opa/reporter/idtheft/.

Gross, Grant. "Banks Crack Down on Cyber-based Account Takeovers," IDG News Service, January 9, 2013, accessed 08/2013, www.networkworld.com/news/2013/010913-banks-crack-down-on-cyber-based-265685.html.

"Identity Theft Impacts," State of California Department of Justice, Office of the Attorney General, accessed 08/2013, http://oag.ca.gov/idtheft.

Note: The statistics cited are from the Javelin Strategy & Research "2012 Identity Fraud Report," released in February 2013.

FTC Compliant Assistant, https://www.ftccomplaintassistant.gov/.

Financial Institution Letter. Guidance for Managing Third-Party Risk FIL-44-2008, June 6, 2008.

Krebs, Brian. "Target: Small Businesses," Krebs on Security Blog, accessed 08/2013, http://krebsonsecurity.com/category/smallbizvictims/.

"PATCO Construction Company v. People's United Bank, United States District Court District of Maine, Case 2:09-cv-00503-DBH," accessed 08/2013, www.goodwinprocter.com/~/media/585506BA9D5C4280996AC20523131EF8.pdf%20.

"PATCO Construction Company v. People's United Bank, United States Court of Appeals for the First Circuit, Case 11-2031," accessed 08/2103, www.wired.com/images_blogs/threatlevel/2012/11/Patco-Appellate-Decision.pdf.

"The Evolution of Bank Information Technology Examinations," *FDIC Supervisory Insights*, Summer 2013, Volume 10, Issue 1, accessed 08/2013, www.fdic.gov/regulations/examinations/supervisory/insights/index.html.

Chapter 14

Regulatory Compliance for the Healthcare Sector

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Explain healthcare-related information security regulatory compliance requirements.
- Understand the components of a HIPAA/HITECH-compliant information security program.
- Prepare for a regulatory audit.
- Know how to respond to an ePHI security incident.
- Write HIPAA-related policies and procedures.

The genesis of healthcare security–related legislation is the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191). The original intent of the HIPAA regulation was to simplify and standardize healthcare administrative processes. Administrative simplification called for the transition from paper records and transactions to electronic records and transactions. The Department of Health and Human Services (HHS) was instructed to develop and publish standards to protect an individual's electronic health information while permitting appropriate access and use of that information by healthcare providers and other entities. On August 14, 2002, the Standards for Privacy of Individually Identifiable Health Information, known as the HIPAA Privacy Rule, was published. The Privacy Rule set limits and conditions on the use and disclosure without patient authorization, and gave patients control over their health information, including the right to examine and obtain a copy of their health records, and to request corrections. The Privacy Rule applies to all formats of protected health information (PHI; for example, paper, electronic, oral). On February 20, 2003, the Security

Standards for the Protection of Electronic Protected Health Information, known as the HIPAA Security Rule, was published. The Security Rule required technical and nontechnical safeguards to protect electronic health information. The corresponding HIPAA Security Enforcement Final Rule was issued on February 16, 2006. Since then, the following legislation has modified and expanded the scope and requirements of the Security Rule:

- 2009 Health Information Technology for Economic and Clinical Health Act (known as the HITECH Act)
- 2009 Breach Notification Rule
- 2013 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (known as the Omnibus Rule)

In this chapter, we will examine the components of the original HIPAA Security Rule, the HITECH Act, and the Omnibus Rule. We will discuss the policies, procedures, and practices that entities need to implement to be considered HIPAA compliant. We will conclude the chapter with a look at incident response and breach notification requirements.

FYI: ISO/IEC 27002:2013 and NIST Guidance

Section 18 of ISO 27002:2013 is dedicated to the Compliance Management domain, which focuses on compliance with local, national, and international criminal and civil laws, regulatory or contractual obligations, intellectual property rights (IPR), and copyrights.

Corresponding NIST guidance is provided in the following documents:

- SP 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security
- SP 800-111: Guide to Storage Encryption Technologies for End User Devices*
- SP 800-52: Guidelines for Selection and Use of Transport Layer Security (TLS) Implementation*
- SP 800-77: Guide to IPSec VPNs*
- SP 800-113: Guide to SSL VPNs*

* Although a number of other NIST publications are applicable, the Department of Health and Human Services specifically refers to the NIST publications for guidance related to data encryption at rest and in motion.

The HIPAA Security Rule

The HIPAA Security Rule focused on safeguarding ***electronic protected health information (ePHI)***, which is defined as individually identifiable health information (IIHI) that is stored, processed, or transmitted electronically. The HIPAA Security Rule applies to covered entities and business associates. ***Covered entities (CEs)*** include healthcare providers, health plans, healthcare clearinghouses, and certain business associates.

- A ***healthcare provider*** is defined as a person or organization that provides patient or medical services, such as doctors, clinics, hospitals, out-patient services and counseling, nursing homes, hospices, pharmacies, medical diagnostic and imaging services, and durable medical equipment providers.
- A ***health plan*** is defined as an entity that provides payment for medical services such as health insurance companies, HMOs, government health plans, or government programs that pay for healthcare such as Medicare, Medicaid, military, and veterans' programs.
- A ***healthcare clearinghouse*** is defined as an entity that processes nonstandard health information it receives from another entity into a standard format.
- ***Business associates*** were initially defined as persons or organizations that perform certain functions or activities that involve the use or disclosure of PHI on behalf of, or provide services to, a CE. Business associate services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial. Subsequent legislation expanded the definition of a business associate to a person or entity that creates, receives, maintains, transmits, accesses, or has the potential to access PHI to perform certain functions or activities on behalf of a CE.

What Is the Objective of the HIPAA Security Rule?

The HIPAA Security Rule established national standards to protect patient records that are created, received, used, or maintained digitally by a CE. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability (CIA) of ePHI. In Chapter 3, "Information Security Framework," we discussed the CIA Triad and defined its elements as follows:

- *Confidentiality* is the protection of information from unauthorized people, resources, and processes.
- *Integrity* is the protection of information or processes from intentional or accidental unauthorized modification.
- *Availability* is the assurance that systems and information are accessible by authorized users when needed.

The framers of the regulations were realists. They understood that these regulations were going to apply to organizations of various sizes and types throughout the country. They were careful not to mandate specific actions. As a matter of fact, many in the healthcare sector have criticized the DHHS for being too vague and not providing enough guidance. The rule says that a CE may use any security measures that allow it to reasonably and appropriately implement the standards and implementation specification, taking into account the following:

- The size, complexity, and capabilities of the CE.
- The CE's technical infrastructure, hardware, and software capabilities.
- The costs of security measures.
- The probability of potential risks.

The standards were meant to be scalable, meaning that they can be applied to a single-physician practice or to a hospital system with thousands of employees. The standards are technology neutral and vendor nonspecific. CEs are expected to choose the appropriate technology and controls for their unique environment.

Enforcement and Compliance

The DHHS Office of Civil Rights (OCR) Authority is responsible for investigating violations and enforcing the Security Rule. In the original rule, civil penalties were limited to $100 per violation and up to $25,000 per year for each requirement violated. As we will discuss later in the chapter, the 2013 Omnibus Rule significantly increased the fines for noncompliance to up to $1,500,000 per violation per year and gave the OCR the power to audit CEs.

The Department of Justice was given the authority to bring criminal action against CEs that wrongly disclose ePHI. Criminal penalties for knowing violations are up to $50,000 and one year in prison, violations committed under false pretenses are up to $100,000 and five years in prison, and offenses committed for commercial or personal gain are up to $250,000 and ten years in prison.

How Is the HIPAA Security Rule Organized?

The Security Rule is organized into five categories: administrative safeguards, physical safeguards, technical safeguards, organizational requirements, and documentation requirements. Within these five categories are standards and implementation specifications. In this context, a standard defines what a CE must do; implementation specifications describe how it must be done.

- ***Administrative safeguards*** are the documented policies and procedures for managing day-to-day operations, the conduct, and access of workforce members to ePHI, as well as the selection, development, and use of security controls.
- ***Physical safeguards*** are the controls used to protect facilities, equipment, and media from unauthorized access, theft, or destruction.

- ***Technical safeguards*** focus on using technical security measures to protect ePHI data in motion, at rest, and in use.
- ***Organizational requirements*** include standards for business associate contracts and other arrangements.
- ***Documentation requirements*** address retention, availability, and update requirements related to supporting documentation, including policies, procedures, training, and audits.

Implementation Specifications

Many of the standards contain implementation specifications. An implementation specification is a more detailed description of the method or approach CEs can use to meet a particular standard. Implementation specifications are either *required* or *addressable.* Where there are no implementation specifications identified for a particular standard, compliance with the standard itself is required.

- A ***required*** implementation specification is similar to a standard, in that a CE must comply with it.
- For ***addressable*** implementation specifications, CEs must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the CE's environment.

"Addressable" does not mean optional, nor does it mean the specification can be ignored. For each of the addressable implementation specifications, a CE must do one of the following:

- Implement the specification if reasonable and appropriate, *or*
- If the entity determines that implementing the specification is not reasonable and appropriate, the entity must document the rationale supporting the decision and either implement an equivalent measure that accomplishes the same purpose or be prepared to prove that the standard can be met without implementing the specification.

What Are the Administrative Safeguards?

The Security Rule defines administrative safeguards as the "administrative actions, policies, and procedures used to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the CE's workforce in relation to the protection of that information." The Administrative Safeguards section incorporates nine standards focusing on internal organization, policies, procedures, and maintenance of security measures that protect patient health information.

The Security Management Process §164.308(a)(1)

The first standard is the foundation of HIPAA compliance. The standard requires a formal security management process, which includes risk management (inclusive of risk analysis), a sanction policy, and ongoing oversight.

Risk management is defined as the implementation of security measures to reduce risk to reasonable and appropriate levels to ensure the CIA of ePHI, protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, and protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the HIPAA Security Rule. The determination of "reasonable and appropriate" is left to the discretion of the CE. Factors to be considered are the size of the entity, the level of risk, the cost of mitigating controls, and the complexity of implementation and maintenance. Per DHHS guidance, the risk management process includes the following activities:

Analysis

- Identify the ePHI that the organization is responsible for protecting.
- Document potential threats and vulnerabilities.
- Determine the likelihood of threat occurrence.
- Determine the potential impact of threat occurrence.
- Determine the level of risk.

Management

- Develop and implement a risk management plan.
- Implement security measures.
- Maintain continuous, reasonable, and appropriate security protections.

The Security Rule does not dictate a specific risk assessment methodology. However, DHHS implementation and training materials refer to using NIST SP 800-30: Risk Management Guide for Information Technology Systems as a guide.

CEs must implement sanction policies for security violations in regard to ePHI. Specially, CEs must have a written policy that clearly states the ramifications for not complying with the Security Rules as determined by the organization.

Implied in this requirement is a formal process to recognize and report security violations. The policy needs to apply to all employees, contractors, and vendors. Sanctions might range from a reprimand to termination. Again, this is left to the discretion of the organization. It is also implied that all employees have not only been made aware of the sanction policy but have been trained and understand what is expected of them in regard to security behavior.

An integral component of risk management is continuous monitoring, review, and evaluation. The expectation here is that the CE has a mechanism in place to review information system activity and that these reports are reviewed regularly. System activity includes network, application, personnel, and administrative activities. Before a review can be implemented, three basic questions must be addressed:

1. *What system activity is going to be monitored?* The short answer: audit logs, access reports, and security incident–tracking reports are the most common methods of tracking system activity.
2. *How is this going to be accomplished?* Generally, using built-in or third-party monitoring/audit tools for operating systems, applications, and devices, as well as incident reporting logs.
3. *Who is going to be responsible for the overall process and results?* This is usually assigned to the security officer. Realistically, the security officer may not have the technical skills to interpret the reports, in which case it needs to be a combination of information technology (IT) staff (either internal or outsource) and the security officer.

Assigned Security Responsibility §164.308(a)(2)

The second standard in the Administrative Safeguards section is Assigned Security Responsibility. There are no separate implementation specifications for this standard. The Security Rule specifically states that the CE must designate an individual as the security officer. The security officer is responsible for overseeing the development of policies and procedures, management and supervision of the use of security measures to protect data, and oversight of personnel access to data. A formal job description should be developed that accurately reflects the assigned security duties and responsibilities. This role should be communicated to the entire organization, including contractors and vendors.

It is important to select a person who can assess effective security and who can serve as a point of contact for security policy, implementation, and monitoring. It should be pointed out that responsibility for compliance does not rest solely with the security officer. Management is still accountable for the actions of the CE. The entire organization is expected to engage in compliance-related activities. The goal is to create a culture of security and compliance.

Workforce Security §164.308(a)(3)

The third standard is Workforce Security. This standard focuses on the relationship between people and ePHI. The purpose of this standard is to ensure that there are appropriate policies, procedures, and safeguards in place in regard to access to ePHI by the entire workforce. The term *workforce* is purposely used instead of *personnel*. ***Personnel*** are generally those on an organization’s payroll. ***Workforce*** includes anyone who does work at or for the organization. In addition to employees and principals, this includes vendors, business partners, and contractors such as maintenance workers. There are three addressable implementation specifications for this standard: implementing procedures for workforce authorization and supervision, establishing a workforce clearance procedure, and establishing workforce termination procedures.

In Chapter 3, we defined ***authorization*** as the process of granting users and systems a predetermined level of access to information resources. In this case, the specification refers to determining who should have access to ePHI and the level of access. Implied in this specification is that the organization has defined roles and responsibilities for all job functions. Larger CEs would be expected to document workforce access, including type of permission, under what circumstances, and for what purposes. A small medical practice may specify that all internal staff need access to ePHI as a normal part of their job.

CEs need to address whether all members of the workforce with authorized access to ePHI receive appropriate clearances. The goal of this specification is that organizations establish criteria and procedures for hiring and assigning tasks—in other words, ensuring that workers have the necessary knowledge, skills, and abilities to fulfill particular roles and that these requirements are a part of the hiring process. As a part of this process, CEs need to determine the type of screening required for the position. This can range from verification of employment and educational references to criminal and credit checks. It was not the intent of Congress to mandate background checks, but rather to require reasonable and appropriate screening prior to access to ePHI.

When an employee's role or a contractor's role in the organization changes or their employment ends, the organization must ensure that their access to ePHI is terminated. Compliance with this specification includes having a standard set of procedures that should be followed to recover access control devices (ID badges, keys, tokens), recover equipment (laptops, PDAs, pagers), and deactivate local and remote network and ePHI access accounts.

Information Access Management §164.308(a)(4)

The fourth standard in the Administrative Safeguards section is Information Access Management. The goal of the Information Access Management standard is to require that CEs have formal policies and procedures for granting access to ePHI. You may be thinking, haven't we already done this? Let's review what the previous standard requires of CEs—to determine what roles, jobs, or positions should have permission to access ePHI, to establish hiring practices for those who may be granted access to ePHI, and to have a termination process to ensure access is disabled when a workforce member is terminated or no longer requires access. This standard addresses the process of authorizing and establishing access to ePHI. There are one required and two addressable implementation specifications in this section: isolating healthcare clearinghouse functions (required but only applies in limited circumstances), implementing policies and procedures to authorize access, and implementing policies and procedures to establish access.

Once an organization has decided what roles need access and who will be filling the roles, the next step is to decide how access will be granted to ePHI. In this standard, we are approaching the question from a policy perspective. Later on we will revisit this question from a technology perspective. The first decision is at what level or levels will access be granted. Options include hardware level, operating system level, application level, and transaction level. Many organizations will choose a hybrid approach. The second decision is the defined basis for granting access. Options here include ***identity-based access*** (by name), ***role-based access*** (by job or function), and ***group-based access*** (by membership). Larger organizations may gravitate toward role-based access because the job may be very well defined. Smaller entities will tend to use identity-based or group-based access because one person may be tasked with multiple roles.

Assuming the organization has made its decisions on access authorization, the next step is to develop policies and procedures to establish, document, review, modify, and, if necessary, terminate a user's access rights to a workstation, transaction, program, or process. What is expected is that each user's rights can be clearly identified. To do so, every user must have a unique identification. Assigned user roles and group membership must be documented. As discussed in Chapter 6, "Human Resources Security," throughout the workforce lifecycle, there needs to be a defined user-provisioning process to communicate changes in status, role, or responsibility.

Security Awareness and Training §164.308(a)(5)

Users are the first line of defense against attack, intrusion, and error. To be effective, they must be trained and then reminded of the imminent dangers. The Security and Awareness Training standard requires that the organization implement a security awareness and training program on specific topics. Implied in this standard is that the organization provides training on the overall security program, policies, and procedures. The type of training provided is up to the organization. The goal is to provide training that is appropriate for the audience. The training program should be documented, and there should be a mechanism for evaluating the effectiveness of the training. In designing and implementing a training program, the entity needs to address immediate compliance requirements, training programs for new users as they begin employment, periodic retraining, and ongoing awareness programs. There are four addressable implementation specifications for this standard: establishing a security awareness program, providing training on malicious software, login monitoring procedures, and password management.

A security awareness program is designed to remind users of potential threats and their part in mitigating the risk to the organization. According to NIST, the purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. Security awareness should be an ongoing campaign. Suggested delivery methods include posters, screen savers, trinkets, booklets, videos, email, and flyers. The campaign should be extended to anyone who interacts with the CEs' ePHI. This includes employees, contractors, and business partners. Security awareness programs are an essential component of maintaining a secure environment. Even the most security conscious federal agency has posters prominently displayed as you walk through a locked door reminding you to check that no one else entered with you and to verify that the door clicked shut behind you!

The implementation specification includes three training topics: password management, login procedures, and malware. These are important topics because the associated threats can be mitigated by user behavior. Users need to understand the importance of safeguarding their authentication credentials (passwords, tokens, or other codes) and the immediacy of reporting a suspected password compromise. Users should also be taught to recognize anomalies related to authentication, including an unusually slow login process, credentials that work intermittently, and being locked out unexpectedly, and to report anomalies even if they seem minor. As we've discussed in earlier chapters, malware (short for *malicious software*) is one of the most significant threats faced by all Internet-connected organizations. Users need to be trained in how to disrupt the malware delivery channel, how to respond to suspicious system behavior, and how to report suspicious incidents.

Security Incident Procedures §164.308(a)(6)

In Chapter 11, "Information Security Incident Management," we defined a security incident as any adverse event whereby some aspect of an information system or information itself is threatened: loss of data confidentiality, disruption of data integrity, disruption, or denial of service. This standard addresses both reporting of and responding to security incidents. Implied in the standard is that the information users and custodians have had the appropriate training as well as the recognition that outside expertise may be required. There is one implementation specification, and it is required.

Security incident reporting is the foundation of a successful response and recovery process. A security incident reporting program has three components: training users to recognize suspicious incidents, implementing an easy-to-use reporting system, and having staff follow through with investigations and report back their findings to the user. Covered entities are required to have documented procedures in place to support a security incident reporting program.

Incident response procedures address by whom, how to, and within what timeframe an incident report should be responded to. Procedures should include an escalation path based on the criticality and severity of the incident. This should include when to contact law enforcement and forensics experts as well as when it is appropriate to contact patients regarding a security breach. All incidents should be documented. This information should then be incorporated into the ongoing risk management process.

Contingency Plans §164.308(a)(7)

The Contingency Plans standard would have been more aptly named the Business Continuity Plan standard. In Chapter 12, "Business Continuity Management," we discussed the components of business continuity management, including emergency preparedness, response, operational contingency, and disaster recovery. This standard is closely tied to those components. The objective of the Contingency Plans standard is to establish (and implement as needed) policies and procedures for responding to an emergency situation that damages systems that contain ePHI or the ability to deliver patient services. What is not stated but implied in the standard is the need for a business continuity team that is responsible for management of the plan. There are three required and two addressable implementation specifications for this standard: Conducting an application and data criticality analysis, establishing and implementing a data backup plan, and establishing and implementing a disaster recovery plan are required. Establishing an emergency mode operation plan and testing and revising procedures are addressable.

The data and criticality analysis specification requires CEs to identify their software applications (data applications that store, maintain, or transmit ePHI) and determine how important each is to patient care or business needs, in order to prioritize for data backup, disaster recovery, and/or emergency operation plans. For example, access to electronic medical records would be critical to providing care. On the other hand, claims processing, while important to the financial health of the entity, does not in the short term affect patient care. In Chapter 12, we referred to this process as a *business impact analysis*.

The data backup specification requires that CEs establish and implement procedures to create and maintain retrievable exact copies of ePHI. This means that all ePHI needs to be backed up on a scheduled basis. The implementation mechanism is left up to the organization. However, the procedures to back up (and restore) the data must be documented and the responsibility to run and verify the backup must be assigned. In addition to verification that the backup job ran successfully, test restores should be conducted regularly. Testing both verifies the media and provides a training opportunity in a low-stress situation. There are few situations more nerve-wracking than that of learning how to restore data in a crisis situation. Backup media should not remain onsite. It should be securely transported offsite. The location where it is stored needs to be secured in accordance with the organization's security policy.

The disaster recovery specification specifically requires that CEs be able to restore any data that has been lost. The initial interpretation is the ability simply to restore data. In actuality, the process is much more complex. Organizations must consider worst-case scenarios. What if the building was not accessible? What if equipment was destroyed? What if the communications infrastructure was unavailable? What if trained personnel were unavailable? A disaster recovery plan should be developed that addresses the recovery of critical infrastructure, including information systems and communications (phone, data, and Internet) as well as restoration of data.

The emergency mode operation specification requires that ePHI (and by extension, the network) be protected from harm during adverse circumstances such as a disaster or emergency situation.

The testing and revision procedures specification requires that organizations implement procedures for periodic testing and revision of contingency plans. As discussed in Chapter 12, plans and procedures are purely theoretical until they are tested. The objective of a testing program is to ensure that plans and procedures are accurate, relevant, and operable under adverse conditions. As important as demonstrating success is uncovering inadequacies.

Evaluation §184.308(a)(8)

The Evaluation standard focuses on developing criteria and metrics for reviewing all standards and implementation specifications for compliance. This standard serves as the sole implementation specification and is required. All CEs need to evaluate their compliance status. This is an ongoing process and should occur both on a scheduled basis (an annual review is recommended but not required) and whenever change drivers warrant reassessment. The evaluation can be conducted internally if the organization has staff appropriately trained for the task. Optionally, third parties can be hired to conduct the assessment and report their findings. Prior to contracting with a third party, the vendor should be required to document credentials and experience with HIPAA compliance. The evaluation should review all five categories of requirements—administrative, physical, technical, organizational, and documentation requirements. The desired outcome of the evaluation is acknowledgment of compliance activities and recommendations for improvement.

There is not a formal certification or accreditation process for HIPAA compliance. There is no organization or person who can put an "official" stamp of approval on the compliance program. The process is one of self-certification. It is left to the organization to determine if its security program and compliance activities are acceptable. If challenged, the organization will need to provide thorough documentation to support its decisions.

Business Associate Contracts and Other Arrangements §164.308(b)(1)

The last standard in the Administrative Safeguards section is Business Associate Contracts and Other Arrangements. The organizational requirements related to this standard are discussed in more detail in §164.314 of the rule, titled "Organizational Policies and Procedures and Documentation." Business associates compliance requirements are further defined in the HITECH Act and the Omnibus Rule, both of which are discussed later in this chapter.

CEs share ePHI for a variety of reasons. The standard states that a CE may permit a business associate to create, receive, maintain, or transmit ePHI on a CE's behalf only if the CE obtains satisfactory assurances that the business associate will appropriately safeguard the information. Services provided by business associates include claim processing or billing, transcription, data analysis, quality assurance, practice management, application support, hardware maintenance, and administrative services.

The required implementation specification requires CEs to document the satisfactory assurances required through a written contract or other arrangement with the business associate that meets the applicable requirements. Implied in this standard is that the CE will establish criteria and procedures for measuring contract performance. Procedures may range from clear lines of communication to onsite security reviews. Of particular importance is a process for reporting security incidents relative to the relationship. If the criteria aren't being met, then a process needs to be in place for terminating the contract. Conditions that would warrant termination should be included in the business associate agreement as well as in performance contracts.

In Practice

HIPAA Administrative Standards Synopsis

All of the standards and implementation specifications found in the Administrative Safeguards section refer to administrative functions, such as policy and procedures that must be in place for management and execution of security measures.

Standard	Implementation Specification
Security Management Process	Risk Analysis Risk Management Sanction Policy Information System Activity Review
Assigned Security Responsibility	Assigned Security Responsibility
Workforce Security	Authorization and/or Supervision Workforce Clearance Procedure Termination Procedures
Information Access Management	Isolating Health Care Clearinghouse Functions Access Authorization Access Establishment and Modification
Security Awareness and Training	Security Reminders Protection from Malicious Software Login Monitoring Password Management
Security Incident Procedures	Response and Reporting
Contingency Plan	Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plans Testing and Revision Procedures Application and Data Criticality Analysis
Evaluation	Evaluation
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement

What Are the Physical Safeguards?

The Security Rule defines physical safeguards as the “physical measures, policies, and procedures to protect a CEs’ electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” Physical safeguards are required at all locations that store, process, access, or transmit ePHI. This requirement extends to the telecommuting or mobile workforce.

Facility Access Controls §164.310(a)(1)

The first physical safeguard standard is Facility Access Controls. ***Facility*** is defined as the physical premises and the interior and exterior of a building. Facility access controls are policies and procedures to limit physical access to ePHI information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. There are four addressable implementation specifications for this standard: creating a facility security plan, implementing access control and validation procedures, keeping maintenance records, and establishing contingency operations. All four implementation specifications are addressable.

The facility security plan specification requires that the safeguards used by the entity to secure the premise and equipment from unauthorized access, tampering, and theft be documented. The most basic control that comes to mind are door locks. Implied in this specification is the need to conduct a risk analysis to identify vulnerable areas. The risk analysis would focus on the building perimeter, interior, and computer room/data centers. Areas that would be examined include entry points such as doors, windows, loading docks, vents, roof, basement, fences, and gates. Based on the outcome of the risk assessment, the facility security plan may include controls such as surveillance monitoring, environmental equipment monitoring, environmental controls (air conditioning, smoke detection, and fire suppression), and entrance/exit controls (locks, security guards, access badges).

Access control and validation procedures specification focuses on the procedures used to ensure facility access to authorized personnel and visitors and exclude unauthorized persons. Facility access controls are generally based on their role or function. These functional or role-based access control and validation procedures should be closely aligned with the facility security plan.

The maintenance records implementation specification requires that CEs document such facility security repairs and modifications, such as changing locks, routine maintenance checks, and installing new security devices. Organizations that lease space should require the owner to provide such documentation.

The establishing contingency operations implementation specification is an extension of the contingency plan requirement in the Administrative Safeguards section. An entity needs to establish procedures to ensure authorized physical access in case of emergency. Generally, these procedures are manual overrides of automated systems. The access control system for a computer room may have been designed to use a swipe card or biometric identification. If the facility were to lose power, these controls would be useless. Assuming that entry into the computer room is required, a contingency or alternate plan would be necessary.

Workstation Use §164.310(b)

The Workstation Use standard addresses the policies and procedures for how workstations should be used and protected. This is generally accomplished by establishing categories of devices (such as wired workstation, wireless workstation, mobile device, and smartphone) and subcategories (such as location) and then determining the appropriate use and applicable safeguard. This standard serves as the sole implementation specification.

Workstation Security §164.310(c)

The Workstation Security standard addresses how workstations are to be physically protected from unauthorized users. Physical safeguards and other security measures should be implemented to minimize the possibility of access to ePHI through workstations. If possible, workstations should be located in restricted areas. In situations where that is not possible, such as exam rooms, workstations should be physically secured (locked) and password-protected with an automatic screen saver. Also, USB ports should be disabled. Shoulder surfing is of particular concern here. Shoulder surfing in its most basic form is when a passerby can view information on another person's computer screen by looking at the monitor or capturing an image using a camera or phone. Workstations located in semi-public areas such as reception desks need to be positioned away from the viewing public. If that is not possible, they should be encased in privacy screens. This standard serves as the sole implementation specification.

Device and Media Controls §164.310(d)(1)

The Device and Media Controls standard requires CEs to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility. Electronic media is defined as "memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card…." This standard covers the proper handling of electronic media, including receipt, removal, backup, storage, reuse, disposal, and accountability. There are two required and two addressable implementation procedures for this standard: Maintaining accountability for hardware and electronic media and developing data backup and storage procedures are required. Implementing reuse policies and procedures, and implementing disposal policies and procedures are addressable.

The objective of the maintaining accountability for hardware and electronic media implementation specification is to be able to account at all times for the whereabouts of ePHI. Implied is that all systems and media that house ePHI have been identified and inventoried. The goal is to ensure that ePHI is not inadvertently released or shared with any unauthorized party. This is easy to understand if you envision a paper medical record (chart). Before the record is allowed to leave the premises, it must be verified that the request came from an authorized party. The removal of the chart is logged and a record kept of the removal. The logs are reviewed periodically to ensure that the chart has been returned. This specification requires the same type of procedures for information stored in electronic form.

The developing data backup and storage procedures specification requires that before moving or relocating any equipment that contains ePHI, a backup copy of the data be created. The objective is to ensure that in case of damage or loss, an exact, retrievable copy of the information is available. Concurrent with this action is the implied requirement that the backup media will be stored in a secure location separate from the original media. This specification protects the availability of ePHI and is similar to the data backup plan implementation specification for the Contingency Plans standard of the Administrative Safeguards, which requires CEs to implement procedures to create and maintain retrievable exact copies of ePHI.

The implementing disposal policies and procedures specification requires that there be a process that ensures that end-of-life electronic media that contains ePHI be rendered unusable and/or inaccessible prior to disposal. As discussed in Chapter 7, "Physical and Environmental Security," options for disposal include disk wiping, degaussing, and physical destruction.

Instead of disposing of electronic media, entities may want to reuse it. The implementing reuse policies and procedures specifications require that there be a process to sanitize the media before reuse or reassignment. Often overlooked are hard drives in workstations or printers that are being recycled either within or outside of the organization. Don't assume that because a policy states that ePHI isn't stored on a local workstation that the drive doesn't need to be cleaned. ePHI is found in the most unexpected of places, including hidden, temporary, cached, and Internet files as well as in metadata.

In Practice

HIPAA Physical Standards Synopsis

The Security Rule's physical safeguards are the physical measures, policies, and procedures to protect electronic information systems, buildings, and equipment.

Standard	Implementation Specification
Facility Access Control	Facility Security Plan Access Control and Validation Procedures Maintenance Records Contingency Operations
Workstation Use	Workstation Use
Workstation Security	Workstation Security
Device and Media Control	Data Backup and Storage Accountability Media Reuse Media Disposal

What Are the Technical Safeguards?

The Security Rule defines technical safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." The Security Rule is vendor neutral and does not require specific technology solutions. A CE must determine which security measures and specific technologies are reasonable and appropriate for implementation in its organization. The basis of this decision making should be a risk analysis.

Technical safeguards include access controls, audit controls, integrity controls, authentication controls, and transmission security. There is a wide range of technology solutions that organizations can choose from to meet the implementation specifications. 45 CFR §164.306(b), the Security Standards: General Rules, Flexibility of Approach, clearly states that entities may take into account the cost of various measures in relation to the size, complexity, and capabilities of the organization. However, it is not permissible for entities to use cost as the sole justification for not implementing a standard.

Access Control §164.312(a)(1)

The intent of the Access Control standard is to restrict access to ePHI to only those users and processes that have been specifically authorized. Implied in this standard are the fundamental security concepts of *deny-all*, *least privilege*, and *need-to-know*. The Access Control standard has two required and two addressable implementation specifications: Requiring unique user identification and establishing emergency access procedures are required. Implementing automatic logoff procedures and encrypting/decrypting information at rest are addressable.

The required unique user identification implementation specification mandates that each user and process be assigned a unique identifier. This can be a name and/or number. The naming convention is at the discretion of the organization. The objective of this specification is accountability. A unique identifier ensures that system activity and access to ePHI can be traced to a specific user or process.

The objective of establishing emergency access procedures is to ensure continuity of operations should normal access procedures be disabled or become unavailable due to system problems. Generally, this would be an administrator or super user account that has been assigned override privileges and cannot be locked out.

The objective of the implementing automatic logoff procedures specification is to terminate a session after a predetermined time of inactivity. The assumption here is that users might leave their workstations unattended, during which time any information their accounts have permission to access is vulnerable to unauthorized viewing. Although the implementation standard incorporates the term "logoff," other mechanisms are acceptable. Examples of other controls include password-protected screen savers, workstation lock function, and disconnection of a session. Based on the risk analysis, it is up to the organization to determine both the "predetermined time of inactivity" as well as the method of termination.

The addressable specification to encrypting and decrypting data at rest is intended to add an additional layer of protection over and above assigned access permissions. NIST defines ***data at rest*** as data that resides in databases, file systems, flash drives, memory, and/or any other structured storage method. Encryption can be resource intensive and costly. The decision to encrypt data at rest should be based on the level of risk as determined by a thorough risk analysis. Regardless, there is no question that mobile devices and media should always be encrypted because the potential for loss, theft, or unauthorized access is high. Both the HITECH Act and the Omnibus Rule refer to unencrypted data as "unsecure data" and require that a breach or potential breach of unsecure data be disclosed.

Audit Controls §164.312(b)

The Audit Controls standard requires implementation of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain ePHI. This standard is closely tied to the administrative standards requiring information system review and security management. This standard serves as the sole implementation specification.

Organizations must have the means available to monitor system activity in order to determine if a security violation has occurred. Audit controls can be automatic, manual, or a combination of both. For example, system logs may run continuously in the background while audit of a specific user activity may need to be manually initiated as the need arises. Most operating systems and applications have at least a minimum level of auditing as part of the feature set. The market is replete with third-party options. The Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. It is the responsibility of the entity to determine reasonable and appropriate audit controls for information systems that contain or use ePHI.

Integrity Controls §164.312(c)(1)

Earlier in this chapter, we defined *integrity* as the protection of information or processes from intentional or accidental unauthorized modification. In a healthcare setting, this is of particular importance because modification could jeopardize patient care. The Integrity Controls standard requires organizations to implement technical controls that protect ePHI from improper alteration or destruction. There is one addressable implementation specification: mechanisms to authenticate ePHI. The specification speaks to electronic mechanisms that corroborate that ePHI has not been altered or destroyed in an unauthorized manner. The most common tools used for verification are file integrity checkers, message digests, and digital signatures.

Person or Entity Authentication §164.312(d)

Authentication is defined as the process of identifying an individual, usually based on a username and password. Authentication is different from *authorization*, which is the process of giving individuals access based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the individual's access rights. The Person or Entity Authentication standard requires verification that a person or process seeking access to ePHI is the one claimed. An entity can be a process or a service. This standard serves as the sole implementation specification.

The earlier Access Control standard required identification for accountability. The Authentication standard requires identification for verification. As we discussed in Chapter 9, "Access Control Management," the process of authentication requires the subject to supply identification credentials. The credentials are referred to as *factors*. There are three categories of factors: knowledge (something the user knows), possession (something a user has), and inherence (something the user is). Single-factor authentication is when only one factor is presented. The most common method of single-factor authentication is the password. Multifactor authentication is when two or more factors are presented. Multilayer authentication is when two or more of the same type of factors are presented. It is up to the CE to decide the appropriate approach. In all cases, users should receive training on how to protect their authentication credentials.

Transmission Security §164.312(e)(1)

The Transmission Security standard states that CEs must implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network. Implied in this standard is that organizations identify scenarios that may result in modification of the ePHI by unauthorized sources during transmission. Based on the assumption that the facility is secure, the focus is on external transmission. There are two addressable implementation specifications: implementing integrity controls and implementing encryption. Just as in the previous integrity control, the objective of the implementing integrity control specification is to protect ePHI from intentional or accidental unauthorized modification. Looking at integrity in this context, the focus is on protecting ePHI in motion. NIST defines ***data in motion*** as data that is moving through a network, including wireless transmission, whether by email or structured electronic interchange. The second implementation standard requires that CEs consider the reasonableness of encrypting ePHI in motion. Conventional wisdom dictates that all ePHI transmitted over a public network be encrypted. Security measures are used in tandem to protect the integrity and confidentiality of data in transit. Examples include virtual private networks (VPNs), secure email products, and application layer protocols such as SSL, SSH, and SFTP.

In Practice

HIPAA Technical Standards Synopsis

The Security Rule technical safeguards are the technology and related policies and procedures that protect ePHI and control access to it.

Standard	Implementation Specification
Access Control	Unique User Identification Emergency Access Procedures Automatic Logoff Encryption and Decryption
Audit Controls	Audit Controls
Integrity	Mechanism to Authenticate ePHI
Person or Entity Authentication	Person or Entity Authentication
Transmission Security	Integrity Controls Encryption

What Are the Organizational Requirements?

The next two standards are categorized as organizational requirements and deal specifically with contracts and other arrangements. The standard provides the specific criteria for written contracts or other arrangements between CEs and business associates. The intent of this standard was to contractually obligate business associates to protect ePHI. The 2013 Omnibus Rule extended HIPAA/HITECH compliance requirements to business associates.

Business Associates Contracts §164.314(a)(1)

Per the Department of Health and Human Services, a *business associate* is a person or entity, other than a member of the workforce of a CE, who performs functions or activities on behalf of, or provides certain services to, a CE that involve access by the business associate to PHI. A business associate also is a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard PHI. Contracts between a covered entity and its business associates must include the following criteria:

- Establish the permitted and required uses and disclosures of PHI by the business associate.

- Provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law.
- Require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to ePHI.
- Require the business associate to report to the CE any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI.
- Require the business associate to disclose PHI as specified in its contract to satisfy a CE's obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings.
- To the extent the business associate is to carry out a CE's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation.
- Require the business associate to make available to DHHS its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the CE for purposes of DHHS determining the CE's compliance with the HIPAA Privacy Rule.
- At termination of the contract, if feasible, require the business associate to return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered CE.
- Require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the business associate with respect to such information.
- Authorize termination of the contract by the CE if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

A CE will be considered out of compliance if the entity knew of a pattern of an activity or practice of a business associate that constituted a material breach or violation of the business associate's obligations, unless the CE took reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the CE must terminate the contract or arrangement, if feasible. If not feasible, the problem must be reported to the DHSS Secretary.

The other arrangements implementation specification is an exception and provides for alternatives to the contractual obligation requirement when both the CE and the business associate are government agencies. Provisions include a memorandum of understanding (MOU) and recognition of statutory obligations.

In Practice

HIPAA Organizational Requirements Synopsis

The Security Rule organizational requirements relate to business associate obligations to protect ePHI in compliance with HIPAA requirements and to report any violation or security incident to the CE.

Standard	Implementation Specification
Business Associate Contracts or Other Arrangements	Business Associate Contracts Other Arrangements

What Are the Policies and Procedures Standards?

The last two standards are categorized as policy and procedure requirements. There are a total of four implementation specifications, all of which are required.

Policies and Procedures §164.316 (a)

CEs are required to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule. This standard serves as the sole implementation specification.

The policies and procedures must be sufficient to address the standards and implementation specifications and must accurately reflect the actual activities and practices of the CE, its staff, its systems, and its business associates. A CE may change its policies and procedures at any time, provided the changes are documented and implemented in accordance with the Documentation standard.

Documentation §164.316(b)(1)

The Documentation standard requires that all policies, procedures, actions, activities, and assessments related to the Security Rule be maintained in written or electronic form. There are three required implementation specifications: time limit, availability, and updates.

CEs are required to retain all documentation related to the Security Rule for a period of six years from the date of creation or the date it was last in effect, whichever is later. This requirement is consistent with similar retention requirements in the Privacy Rule.

Documentation must be easily accessible to all persons responsible for implementing the procedures to which the documentation pertains. This would include security professionals, systems administrators, human resources, contracts, facilities, legal, compliance, and training.

Documentation must be reviewed periodically and updated as needed in response to operational, personnel, facility, or environmental changes affecting the security of ePHI. Particular attention should be paid to version control.

In Practice

Policies, Procedures, and Documentation Requirements Synopsis

The policies, procedures, and documentation requirements relate to the implementation and maintenance of CEs' HIPAA-related security plans, policies, and procedures.

Standard	Implementation Specification
Documentation	Time Limit Availability Updates

The HITECH Act and the Omnibus Rule

The Health Information Technology for Economic and Clinical Health Act (known as the HITECH Act) is part of the American Recovery and Reinvestment Act of 2009 (ARRA). The ***HITECH Act*** amended the Public Health Service Act (PHSA) with a focus on improving healthcare quality, safety, and efficiency through the promotion of health information technology. The HITECH Act dedicated over $31 billion in stimulus funds for healthcare infrastructure and the adoption of electronic health records (EHR), including funding for the meaningful use incentive programs. The HITECH Act also widened the scope of privacy and security protections available under HIPAA.

The Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules (known as the Omnibus Rule) was published January 25, 2013 with a compliance date of September 23, 2013. The ***Omnibus Rule*** finalizes the Privacy, Security, and Enforcement Rules that were introduced in HITECH, modifies the Breach Notification Rule, and expands the definition of "business associates."

Prior to HITECH and the Omnibus Rule, the government had little authority to enforce the HIPAA regulations. Complicating matters was the fact that entire industry segments that stored, processed, transmitted, and accessed ePHI were not explicitly covered by the law. The 2013 Final Omnibus Rule made significant changes in coverage, enforcement, and patient protection in the following ways:

- Expanding the definition of "business associates."
- Extending compliance enforcement to business associates and subcontractors of business associates.

- Increasing violation penalties with potential fines, ranging from $25,000 to as much as $1.5 million.
- Including provisions for more aggressive enforcement by the federal government and requiring the DHHS to conduct mandatory audits.
- Granting explicit authority to state Attorneys General to enforce HIPAA Rules and to pursue HIPAA criminal and civil cases against HIPAA CEs, employees of CEs, or their business associates.
- Defining specific thresholds, response timelines, and methods for security breach victim notification.

What Changed for Business Associates?

The original Security Rule defined a *business associate* as a person or organization that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a CE. The final rule amends the definition of a *business associate* to mean a person or entity that creates, receives, maintains, transmits, or accesses PHI to perform certain functions or activities on behalf of a CE. The accompanying guidance further defines *access* and specifies that if a vendor has access to PHI in order to perform its duties and responsibilities, regardless of whether the vendor actually exercises this access, the vendor is a business associate.

Subcontractors and Liability

Effective September 2013, subcontractors of business associates that create, receive, maintain, transmit, or access PHI are considered business associates. The addition of subcontractors means that all HIPAA security, privacy, and breach notification requirements that apply to direct contract business associates of a CE also apply to all downstream service providers. CEs are required to obtain "satisfactory assurances" that their ePHI will be protected as required by the rules from their business associates, and business associates are required to get the same from their subcontractors. Business associates are directly liable and subject to civil penalties (discussed in the next section) for failing to safeguard ePHI in accordance with the HIPAA Security Rule.

As reported in the January 23, 2013 Federal Register, the DHHS estimates that in the United States there one to two million business associates and an unknown number of subcontractors. Expanding the number of businesses subject to HIPAA regulations is so significant that it could alter the American security landscape.

What Has Changed with Enforcement?

The DHHS OCR was tasked with enforcing the original HIPAA privacy and security rule. However, enforcement was limited. Prior to the HITECH Act, OCR was permitted to assess civil penalties of $100 per violation of the Privacy and Security Rules, up to $25,000 for violations of each requirement during a calendar year. A CE could also bar the imposition of a civil money penalty by demonstrating that it did not know that it violated the HIPAA rules. The HITECH Act increased the amounts of the civil penalties that may be assessed and distinguishes between the types of violations. Additionally, a CE can no longer bar the imposition of a civil money penalty for an unknown violation unless it corrects the violation within 30 days of discovery. Table 14.1 lists the violation categories, per-violation fine, and annual maximum penalty as of September 2013.

TABLE 14.1 HIPAA/HITCH Security Rule Violation Penalties

Violation Category	Per Violation	Annual Maximum
Did Not Know	$100–$50,000	$1,500,000
Reasonable Cause	$1,000–$50,000	$1,500,000
Willful Neglect – Corrected	$10,000–$50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$1,500,000

The HITECH Act did not change the criminal penalties that may be assessed for violations of the Privacy and Security Rules. Those penalties remain $50,000 and one year in prison for knowing violations, $100,000 and five years in prison for violations committed under false pretenses, and $250,000 and ten years in prison for offenses committed for commercial or personal gain. Under the HITECH Act, criminal actions may be brought against anyone who wrongly discloses PHI, not just CEs or their employees. Also, the Act gives the DHHS OCR (in addition to the Department of Justice) the authority to bring criminal actions against these individuals.

State Attorneys General

The HITECH Act expanded the enforcement of HIPAA by granting authority to State Attorneys General to bring civil actions and obtain damages on behalf of state residents for violations of HIPAA Privacy and Security Rules. In January 2010, Connecticut Attorney General Richard Blumenthal became the first to exercise this power when he filed a lawsuit against Health Net of Connecticut, alleging the company failed to secure patient medical records and financial information prior to a security breach. In July 2010, Blumenthal announced a $250,000 settlement.

The Act also allowed for prosecution of business associates. In January 2012, Minnesota Attorney General Lori Swanson became the first to charge a business associate with a HIPAA violation. On July 30, 2012 her office announced a settlement that required Accretive Health to stop doing business in

Minnesota for two years and to pay approximately $2.5 million to the state, a portion of which will be used to compensate patients.

Proactive Enforcement

Prior to HITECH, the DHHS OCR would investigate potential security of privacy violations if they received a complaint. HITECH requires proactive enforcement including the mandate to perform periodic audits of CE and business associate compliance with the HIPAA Privacy, Security, and Breach Notification Rules. In 2011, OCR launched a pilot audit program. Based on funding requests, it is anticipated that audits will begin in 2014.

FYI: DHHS Settles with Health Plan in Photocopier Breach Case (August 14, 2013)

Under a settlement with the U.S. DHHS, Affinity Health Plan, Inc., will settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules for $1,215,780. Affinity Health Plan is a not-for-profit managed care plan serving the New York metropolitan area.

Affinity filed a breach report with the DHHS OCR on April 15, 2010, as required by the HITECH Act. The HITECH Breach Notification Rule requires HIPAA-covered entities to notify DHHS of a breach of unsecured PHI. Affinity indicated that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by Affinity. CBS informed Affinity that the copier that Affinity had used contained confidential medical information on the hard drive.

Affinity estimated that up to 344,579 individuals may have been affected by this breach. OCR's investigation indicated that Affinity impermissibly disclosed the PHI of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives. In addition, the investigation revealed that Affinity failed to incorporate the electronic ePHI stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

"This settlement illustrates an important reminder about equipment designed to retain electronic information: Make sure that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent," said OCR Director Leon Rodriguez. "HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information."

In addition to the $1,215,780 payment, the settlement includes a corrective action plan requiring Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent, and to take certain measures to safeguard all ePHI.

Source: DHHS Office of Civil Rights, August 14, 2013

What Are the Breach Notification Requirements?

The original Security Rule did not include standards related to incident response and security breaches. The HITECH Act established several notification requirements for CEs and business associates. In 2009, the DHHS issued the Breach Notification Rule. The Omnibus Rule made significant changes to the Breach Notification Rule's definition of "breach" and provided guidance on a number of Breach Notification Rule requirements.

Safe Harbor Provision

For the purposes of breach notification, ePHI is considered to be "secure" if it meets the following criteria:

- ePHI has been rendered unusable, unreadable, or indecipherable using an NIST-approved encryption method.
- The decryption tools are stored on a device or at a location separate from the data they are used to encrypt or decrypt.

If a CE or business associate "secures" ePHI, as noted, and an unauthorized use or disclosure is discovered, the breach notice obligations do not apply. This exception is known as the Safe Harbor Provision. The term *secure* ePHI is specific to the Safe Harbor Provision and does not in any way modify an entity's obligation to comply with the HIPAA Security Rule.

Breach Definition

Per DHHS, "impermissible acquisition, access, or use or disclosure of *unsecured* PHI is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised." To demonstrate that there is a low probability that a breach compromised ePHI, a CE or business associate must perform a risk assessment that addresses the following minimum standards:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom the disclosure was made, whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

Breach notification is not required if a CE or business associate concludes through a documented risk assessment that a low probability exists that the PHI has been compromised. Risk assessments are subject to review by federal and state enforcement agencies.

Breach Notification Requirements

CEs are required to notify individuals whose “unsecured ePHI” has been breached (unless excepted by a risk assessment). This is true even if the breach occurs through or by a business associate. The notification must be made without unreasonable delay and no later than 60 days after the discovery of the breach. The CE must also provide notice to “prominent media outlets” if the breach affects more than 500 individuals in a state or jurisdiction. The notice must include the following information:

- A description of the breach, including the date of the breach and date of discovery
- The type of PHI involved (such as full name, social security number, date of birth, home address, or account number)
- Steps individuals should take to protect themselves from potential harm resulting from the breach
- Steps the CE is taking to investigate the breach, mitigate losses, and protect against future breaches
- Contact procedures for individuals to ask questions or receive additional information, including a toll-free telephone number, email address, website, or postal address

CEs must notify DHHS of all breaches. Notice to DHHS must be provided immediately for breaches involving more than 500 individuals and annually for all other breaches. CEs have the burden of demonstrating that they satisfied the specific notice obligations following a breach, or, if notice is not made following an unauthorized use or disclosure, that the unauthorized use or disclosure did not constitute a breach.

Summary

The intent of the original HIPAA Security Rule and subsequent legislation was to protect patient health information from unauthorized access, disclosure and use, modification, and disruption.

The legislation was groundbreaking, yet many viewed it as another unfunded government mandate. Since adoption, the need to protect ePHI has become self-evident.

The HIPAA Security Rule and subsequent legislation applies to covered entities (CEs). CEs include healthcare providers, health plans, healthcare clearinghouses, and certain business associates. The Security Rule is organized into five categories: administrative safeguards, physical safeguards, technical safeguards, organizational requirements, and documentation requirements. Within these five categories are standards and implementation specifications. In this context, a standard defines what a CE must do; implementation specifications describe how it must be done. The rule says that a CE may use any security measures that allow it to reasonably and appropriately implement the standards and implementation specification, taking into account the size, complexity, and capabilities of the CE, the cost of the security measures, and the threat environment. The standards were meant to be scalable, meaning that they can be applied to a single-physician practice or to an organization with thousands of employees. The standards are technology neutral and vendor nonspecific. CEs are expected to choose the appropriate technology and controls for their unique environments.

There was minimal enforcement power associated with the original regulations. Subsequent legislation (HITECH and the Omnibus Rule) included provisions for aggressive civil and criminal enforcement by the Department of Health and Human Services (DHHS) and the Department of Justice. Fines were increased to up to $1.5 million dollars annually per violation category. Authority was granted to State Attorneys General to bring civil actions and obtain damages on behalf of state residents for violations of HIPAA Privacy and Security Rules. Recognizing the right of patients to know when their information was compromised, the Omnibus Rule codifies required incident response and breach notification requirements.

The HIPAA/HITECH/Omnibus requirements mirror information security best practices. Implementations benefit both providers and patients. Providers are protecting valuable information and information assets. Patients have peace of mind knowing that their trust is being honored.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. Which of the following statements best describes the intent of the initial HIPAA legislation adopted in 1996?

   A. The intent of the initial HIPAA legislation was to simplify and standardize the healthcare administrative process.

   B. The intent of the initial HIPAA legislation was to lower healthcare costs.

   C. The intent of the initial HIPAA legislation was to encourage electronic record sharing between healthcare providers.

   D. The intent of the initial HIPAA legislation was to promote the continued use of paper-based patient records.

2. Which of the following statements best describes the intent of the Security Rule published in 2003?

   A. The intent of the Security Rule was to detail privacy practices.

   B. The intent of the Security Rule was to establish breach notification procedures.

   C. The intent of the Security Rule was to publish standards to protect ePHI.

   D. The intent of the Security Rule was to assign enforcement responsibilities.

3. In addition to healthcare providers, HIPAA/HITECH regulations apply to __________.

   A. medical insurance companies

   B. pharmacies

   C. business associates

   D. All of the above

4. Which of the following statements is *not* true?

   A. HIPAA is technology neutral.

   B. HIPAA is vendor specific.

   C. HIPAA documentation must be saved for six years.

   D. HIPAA is scalable.

5. Which of the following federal agencies is responsible for HIPAA/HITECH administration, oversight, and enforcement?

   A. Department of Health and Human Services

   B. Department of Energy

   C. Department of Commerce

   D. Department of Education

6. Which of the following is *not* a HIPAA/HITECH Security Rule category?

   A. Documentation

   B. Compliance

   C. Physical

   D. Technical

7. Which of the following statements is true?

   A. All implementation specifications are required.

   B. All implementation specifications are optional.

   C. Implementation specifications are either required or addressable.

   D. Addressable specifications are optional.

8. Which of the following statements best defines a business associate?

   A. A business associate is a person or organization that creates, stores, processes, accesses, or transmits data on behalf of the CE.

   B. A business associate is a healthcare provider with whom patient information is shared in the course of treatment.

   C. A business associate is an employee who creates, stores, processes, or transmits data on behalf of the CE.

   D. A business associate is a person or organization that provides any service to the CE.

9. In the context of HIPAA/HITECH, which of the following is *not* a factor to be considered in the determination of "reasonable and appropriate" security measures?

   A. Size of the CE

   B. Level of risk

   C. Geographic location of the CE

   D. Complexity of implementation

10. The Security Rule does not dictate a specific risk assessment methodology; however, the Department of Health and Human Services implementation and training guidance references which of the following methodologies?

- **A.** NIST 800-30: Risk Management Guide for Information Technology Systems
- **B.** OCTAVE
- **C.** FAIR
- **D.** ISO 27002:2013

11. Which of the following statements is true of the role of a HIPAA Security Officer?

- **A.** The role of a HIPAA Security Officer is optional.
- **B.** The role of a HIPAA Security Officer can be performed by a committee.
- **C.** The role of a HIPAA Security Officer is accountable by law for compliance.
- **D.** The role of a HIPAA Security Officer must be assigned to a designated individual.

12. Which of the following statements best defines authorization?

- **A.** Authorization is the process of positively identifying a user or system.
- **B.** Authorization is the process of granting users or systems a predetermined level of access to information resources.
- **C.** Authorization is the process of determining who accessed a specific record.
- **D.** Authorization is the process of logging the access and usage of information resources.

13. Which of the following statements is false?

- **A.** Identity-based access is granted by username.
- **B.** Role-based access is granted by job or function.
- **C.** Group-based access is granted by membership.
- **D.** Clinical-based access is granted by patient name.

14. Which of the following would be considered an optional topic for workforce security training?

- **A.** Malware protection
- **B.** Login procedures
- **C.** Organizational HIPAA compliance penalties
- **D.** Password management

15. Users should be trained to recognize and _________ a potential security incident.

    A. report
    B. contain
    C. recover from
    D. eradicate

16. Which of the following statements is true of HIPAA compliance?

    A. HIPAA certification is granted by DHHS.
    B. HIPAA accreditation is granted by the Joint Commissions for Hospital Accreditation (JCAHO).
    C. There is no formal HIPAA/HITECH certification or accreditation process.
    D. CEs must complete an annual self-assessment and submit it to the Centers for Medicare and Medicaid Services (CMS).

17. Which of the following statements is true of a business associate's HIPAA/HITECH compliance requirements?

    A. A business associate's HIPAA/HITECH compliance requirements are the same as a healthcare provider.
    B. A business associate's HIPAA/HITECH compliance requirements are limited to what is in the BA agreement.
    C. A business associate's HIPAA/HITECH compliance requirements are not as stringent as those of a healthcare provider.
    D. A business associate's HIPAA/HITECH compliance requirements are exempt if the organization's annual gross revenue is less than $500,000.

18. According to the workstation security standard, when users leave their workstation unattended, they should _____________.

    A. do nothing
    B. lock the workstation
    C. log out
    D. turn off their monitor

19. Which of the following is *not* an acceptable end-of-life disposal process for media that contains ePHI?

    A. Permanently wipe it
    B. Shred it
    C. Recycle it
    D. Crush it

20. Granting the minimal amount of permissions necessary to do a job reflects the security principle of ___________.

    A. Need-to-know
    B. Deny all
    C. Allow some
    D. Least privilege

21. Both the HITECH Act and the Omnibus Rule refer to “unsecure data,” which means data __________.

    A. in motion
    B. with weak access controls
    C. that is unencrypted
    D. stored in the cloud

22. Which of the following protocols/mechanisms cannot be used for transmitting ePHI?

    A. SSL
    B. SFTP
    C. Encrypted email
    D. HTTP

23. HIPAA-related documentation must be retained for a period of ______ years from the date of creation or the date it was last in effect, whichever is later.

    A. two
    B. four
    C. six
    D. eight

24. Which of the following changes was *not* introduced by the Omnibus Rule?

    A. The Omnibus Rule expanded the definition of a business associate.
    B. The Omnibus Rule explicitly denied enforcement authority to State Attorneys General.
    C. The Omnibus Rule increased violation penalties.
    D. The Omnibus Rule defined breach notification requirements.

25. Effective September 2013, subcontractors of business associates _____________.

    A. are considered business associates
    B. are granted limited liability
    C. are not considered a covered entity
    D. are exempt from HIPAA/HITECH regulations if they are considered a small business

26. Which of the following is *not* a Security Rule violation category?

- **A.** Did not know
- **B.** Did not cause
- **C.** Willful neglect – corrected
- **D.** Willful neglect – not corrected

27. The “safe harbor” provision applies to __________.

- **A.** encrypted data
- **B.** key management
- **C.** dual control
- **D.** de-identified data

28. Which of the following is *not* required to be included in a breach notification?

- **A.** A description of the breach
- **B.** The type of ePHI involved
- **C.** Contact information for questions pertaining to the incident
- **D.** Who was responsible for the breach

29. A HIPAA standard defines what a covered entity must do; implementation specifications ____________________________.

- **A.** describe the technology that must be used
- **B.** describe how it must be done and/or what it must achieve
- **C.** describe who must do it
- **D.** describe the tools that must be used

30. Subsequent legislation increased the maximum fines for HIPAA/HITECH violations to ______________________.

- **A.** up to $50,000 annually per violation category
- **B.** up to $100,000 annually per violation category
- **C.** up to $1,000,000 annually per violation category
- **D.** up to $1,500,000 annually per violation category

EXERCISES

EXERCISE 14.1: Understanding the Difference Between Privacy and Security

1. Explain the difference between the intent of the HIPAA Privacy and HIPAA Security Rules.
2. Which of the security principles—confidentiality, integrity, and/or availability—does the Privacy Rule apply to?
3. Which of the security principles—confidentiality, integrity, and/or availability—does the Security Rule apply to?

EXERCISE 14.2: Understanding Covered Entities

1. In your geographic area, identify a healthcare provider organization that is subject to HIPAA Security Rule regulations.
2. In your geographic area, identify a business associate that is subject to HIPAA Security Rule regulations.
3. In your geographic area, identify either a health plan or a healthcare clearinghouse that is subject to HIPAA Security Rule regulations.

EXERCISE 14.3: Identifying Key Factors for HIPAA/HITECH Compliance

1. Explain why it is important to maintain an inventory of ePHI.
2. Explain why it is important to conduct HIPAA-related risk assessments.
3. Explain why it is important to obtain senior management support.

EXERCISE 14.4: Developing Security Education Training and Awareness

1. Senior leadership needs to be educated on HIPAA/HITECH requirements. Research and recommend a conference they should attend.
2. A HIPAA security officer needs to stay informed on compliance issues. Research and recommend a peer organization to join, a publication to subscribe to, or an online forum to participate in.
3. The workplace needs to be trained on login monitoring, password management, malware, and incident reporting. Research and recommend an online training program.

EXERCISE 14.5: Creating Documentation Retention and Availability Procedures

1. All HIPAA-related documentation must be retained for a minimum of six years. This includes policies, procedures, contracts, and network documentation. Assuming you will revise the documentation, devise a standard version control procedure.
2. Recommend a way to store the documentation.
3. Recommend a secure, efficient, and cost-effective way to make the documentation available to appropriate personnel.

PROJECTS

PROJECT 14.1: Creating a HIPAA Security Program Manual Outline

You have been tasked with designing a HIPAA security program manual.

1. Write a manual for any one of the following CEs:
   - A 100-bed hospital in a metropolitan location.
   - A consortium of three nursing homes. The nursing homes share administrative and clinical staff. They are all connected to the same network.
   - A multi-specialty medical practice consisting of 29 physicians.
2. Write an introduction to the manual explaining what the HIPAA Security Rule is and why compliance is required.
3. Design a table of contents (TOC). The TOC should correspond to the regulations.
4. For each entry in the TOC, assign development of the corresponding policy or procedure to a specific role in the organization (for example, human resources, building maintenance).

PROJECT 14.2: Assessing Business Associates

A business associate is a person or entity that creates, receives, maintains, transmits, accesses, or has the potential to access PHI to perform certain functions or activities on behalf of a CE.

1. How did HITECH and the Omnibus Rule impact business associates?
2. Identify a "business associate" organization either online or locally. Locate any policies or statements that lead you to believe that they recognize their regulatory obligations. What type of due diligence should a CE conduct in order to ascertain HIPAA/HITECH compliance?
3. Find an example of business associate organizations that were charged by either the FTC or a State Attorney General with a HIPAA/HITECH violation.

PROJECT 14.3: Developing a HIPAA Training Program

HIPAA requires that all workforce members receive annual training related to safeguarding ePHI. You have been tasked with developing an instructor-led training module. Your topic is "Disrupting the Malware Distribution Channel."

1. Develop and deliver a training presentation (and post-training quiz) on the topic. The presentation should be at least ten minutes long. It should be interactive and engage the attendees.
2. Have participants complete the quiz. Based on the results, evaluate the effectiveness of the training.
3. Prepare a security awareness infographic about malware and incident reporting. The purpose of the infographic is to reinforce the training lesson.

Case Study

The Advocate Medical Group ePHI Breach

Advocate Medical Group is the largest Chicago physician group, with more than 1,000 doctors and 200 locations. On July 15, 2013 four unencrypted computers—containing data for more than four million patients—were stolen from the Advocate Medical Group of Chicago administrative building in Park Ridge, Illinois. The information contained on the computers included patients' addresses, dates of birth, names, and social security numbers. Affected patients include those who received treatment as far back as the 1990s. In addition, the computers contained clinical information, such as health insurance data, medical diagnoses, and record numbers.

1. Based on HIPAA/HITECH/Omnibus Rule regulations, was Advocate Medical Group required to notify patients? Explain your answer.
2. Did Advocate Medical Group make any public statements?
3. Did Advocate Medical Group notify patients?
4. Do State Data Breach Notification laws apply to this event?
5. What steps could Advocate Medical Group have taken to prevent or minimize the impact of the data breach?
6. Has there been any enforcement action taken or fines levied against Advocate Medical Group?

References

Regulations Cited

"45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule," Federal Register, Vol. 68, No. 34, February 20, 2003, Department of Health and Human Services.

"45 CFR Parts 160 and 164 (19006-19010): Breach Notification Guidance," Federal Register, Vol. 74, No. 79, April 27, 2009, Department of Health and Human Services.

"Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules 45 CFR Parts 160 and 164 Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule," Federal Register, Vol. 78, No. 17, January 25, 2013.

Other References

"1 – Security 101 for Covered Entities," HIPAA Security Series, Department of Health and Human Services, Volume 2 / Paper 1, Rev 3/2007.

"2 – Security Standards, Administrative Safeguards," HIPAA Security Series, Department of Health and Human Services, Volume 2 / Paper 2, Rev 3/2007.

"3 – Security Standards, Physical Safeguards," HIPAA Security Series, Department of Health and Human Services, Volume 2 / Paper 3, Rev 3/2007.

"4 – Security Standards, Technical Safeguards," HIPAA Security Series, Department of Health and Human Services, Volume 2 / Paper 2, Rev 3/2007.

"6 – Basics of Risk Analysis and Risk Management," HIPAA Security Series, Department of Health and Human Services, Volume 2 / Paper 6, Rev 3/2007.

"Addressing Encryption of Data at Rest in the HIPAA Security Rule and EHR Incentive Program Stage 2 Core Measures," Healthcare Information and Management Systems Society, December 2012.

Alston & Bird, LLP. "Overview of HIPAA/HITECH Act Omnibus Final Rule Health Care Advisory," January 25, 2013, accessed 09/2013, www.alston.com/advisories/healthcare-hipaa/hitech-act-omnibus-finalrule.

"Certification and HER Incentives, HITECH ACT," accessed 09/2013, www.healthit.gov/policy-researchers-implementers/hitech-act-0.

"Guide to Privacy and Security of Health Information," Office of the National Coordinator for Health Information Technology, Version 1.2, 060112.

Foley Lardner, LLP, " Minnesota Attorney General Reaches First Settlement with Business Associate Under HITECH Act," Legal News: Health Care, August 2, 2012, accessed 9/2013, www.foley.com/minnesota-attorney-general-reaches-first-settlement-with-business-associate-under-hitech-act-08-02-2012/.

"HHS Strengthens HIPAA Enforcement," accessed 09/2013, www.hhs.gov/news/press/2009pres/10/20091030a.html.

"HIPAA Omnibus Final Rule Information," accessed 09/2013, http://hipaa-hitech-center.com/hipaa-omnibus-final-rule/.

"HIPAA Omnibus Rule Summary," accessed 09/2013, http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php.

"HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information," American Medical Association, 2010.

"HIPAA Timeline," accessed 10/2013, www.hipaaconsultant.com/hipaa-timeline.

McDermott Will & Emery, LLP. "New HIPAA Regulations Affect Business Associates and Subcontractors," February 11, 2013, accessed 09/2013, www.mwe.com/New-HIPAA-Regulations-Affect-Business-Associates-and-Subcontractors-02-11-2012/.

Monegain, Bernie. “Connecticut AG sues Health Net over security breach,” Healthcare IT News January 12, 2010, accessed 09/2013, www.healthcareitnews.com/news/connecticut-ag-sues-health-net-over-security-breach.

McDermott Will & Emery, LLP. “OCR Issues Final Modifications to the HIPAA Privacy, Security, Breach Notification and Enforcement Rules to Implement the *HITECH* Act,” February 20, 2013, accessed 10/2013, www.mwe.com/OCR-Issues-Final-Modifications-to-the-HIPAA-Privacy-Security-Breach-Notification-and-Enforcement-Rules-to-Implement-the-HITECH-Act.

Monegain, Bernie. “Connecticut AG fines Health Net $250,000 for data security violations,” Healthcare IT News, July 7, 2010, accessed 09/2013, www.healthcarefinancenews.com/news/connecticut-ag-fines-health-net-250000-data-security-violations.

“The HITECH ACT,” accessed 09/2013, www.hipaasurvivalguide.com/hitech-act-summary.php.

“The Privacy Rule,” U.S. Department of Health and Human Services, accessed 09/2013, www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule.

Chapter 15

PCI Compliance for Merchants

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to do the following:

- Describe the PCI Data Security Standard framework.
- Recognize merchant responsibilities.
- Explain the 12 top-level requirements.
- Understand the PCI DSS validation process.
- Implement practices related to PCI compliance.

Between 2008 and 2014, $127 billion dollars worth of credit, debit, and prepaid card transactions were processed. The sheer volume of transactions makes the payment card channel an attractive target for cybercriminals.

FYI: Consumer Credit, Debit, and ATM Card Liability Limits

According to the Federal Trade Commission, the percentage of Americans who have been victims of credit card fraud is 10% and debit card fraud is 7%.

Although the median amount of fraud is $399, actual consumer liability is limited by federal law. The balance of the loss is borne by the merchant, credit card processor, and the issuing bank.

The Fair Credit Billing Act (FCBA) and the Electronic Fund Transfer Act (EFTA) govern credit card, debit card, and ATM liability if a card is lost or stolen.

Under the FCBA, the maximum liability for unauthorized credit card use is $50. However, if the consumer reports a lost card before the credit card is used, the consumer is not responsible for any unauthorized charges. If a credit card number is stolen, but not the card, the consumer is not liable.

Under the EFTA, debit and ATM card liability depends on how quickly the loss or theft is reported. If the card is reported as lost or stolen before any unauthorized charges are made, the consumer is not responsible for any unauthorized charges. If the card is reported within two days after the consumer learns of the loss or theft, the consumer liability is limited to $50. If the card is reported more than two days but less than 60 days after the consumer learns of the loss or theft, the consumer liability is limited to $500. If the card is reported as lost or stolen more than 60 days after a bank statement is sent, the consumer bears all liability.

In order to protect cardholders against misuse of their personal information and to minimize payment card channel losses, the major payment card brands—Visa, MasterCard, Discover, JCB International, and American Express—formed the Payment Card Industry Security Standards Council and developed the Payment Card Industry Data Security Standard (PCI DSS). On December 15, 2004, the Council released version 1.0 of the PCI DSS. Version 2.0 was released in October 2010 and version 3.0 was released in November 2013. The payment card brands can levy fines and penalties against organizations that do not comply with the requirements and/or revoke their authorization to accept payment cards.

In this chapter, we are going to examine the PCI DSS, version 3.0. Although designed for a specific constituency, the requirements can serve as a security blueprint for any organization.

Protecting Cardholder Data

To counter the potential for staggering losses, the payment card brands contractually require all organizations that store, process, or transmit cardholder data and/or sensitive authentication data comply with the PCI DSS. PCI DSS requirements apply to all system components where *account data* is stored, processed, or transmitted.

As shown in Table 15.1, ***account data*** consists of cardholder data plus sensitive authentication data. ***System components*** are defined as any network component, server, or application that is included in, or connected to, the cardholder data environment. The ***cardholder data environment*** is defined as the people, processes, and technology that handle cardholder data or sensitive authentication data.

TABLE 15.1 Account Data Elements

Cardholder Data Includes…	Sensitive Authentication Data Includes…
Primary account number (PAN)	Full magnetic stripe data or equivalent data on a chip
Cardholder name	CAV2/CVC2/CVV2/CID
Expiration date	PINs/PIB blocks
Service code	

Per the standards, the primary account number (PAN) must be stored in an unreadable (encrypted) format. Sensitive authentication data may never be stored post-authorization, even if encrypted.

The PAN is the defining factor in the applicability of PCI DSS requirements. PCI DSS requirements apply if the PAN is stored, processed, or transmitted. If the PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply. If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the cardholder data environment, they too must be protected.

Per the standards, the PAN must be stored in an unreadable (encrypted) format. Sensitive authentication data may never be stored post-authorization, even if encrypted.

Figure 15.1 shows the following elements located on the front of a credit card:

1. Embedded microchip. The microchip contains the same information as the magnetic stripe. Most non-U.S. cards have the microchip instead of the magnetic stripe. Some U.S. cards have both for international acceptance.
2. Primary account number (PAN).
3. Expiration date.
4. Cardholder name.

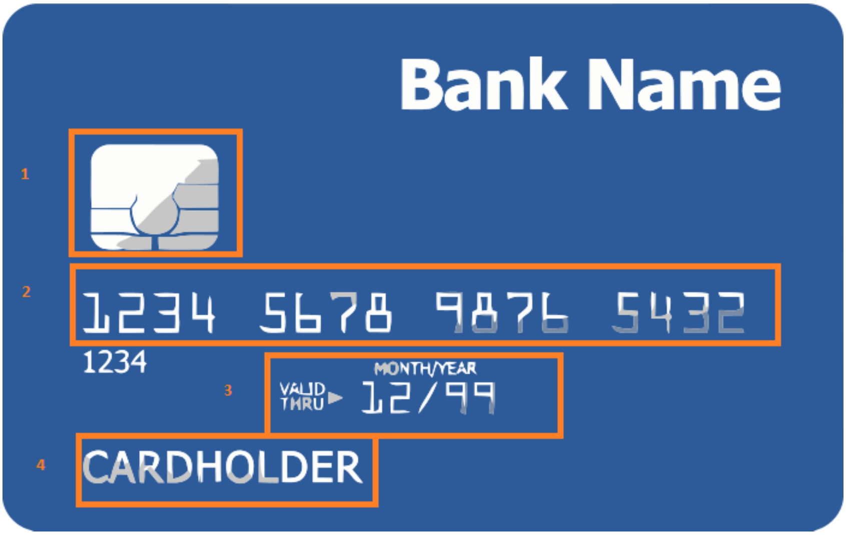


FIGURE 15.1 The elements of the front of a credit card.

Figure 15.2 shows the following elements on the back of a credit card:

1. Magnetic stripe (mag stripe)—The magnetic stripe contains encoded data required to authenticate, authorize, and process transactions.
2. CAV2/CID/CVC2/CVV2—All refer to card security codes for the different payment brands.

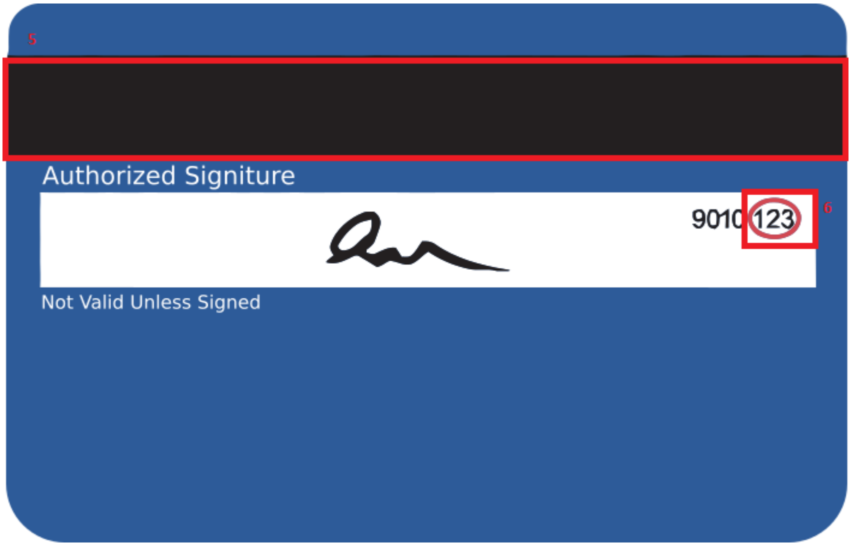


FIGURE 15.2 The elements of the back of a credit card.

Eliminating the collection and storage of unnecessary data, restricting cardholder data to as few locations as possible, and isolating the cardholder data environment from the rest of the corporate network is strongly recommended. Physically or logically segmenting the cardholder data environment reduces the PCI scope, which in turn reduces cost, complexity, and risk. Without segmentation, the entire network must be PCI compliant. This can be burdensome because the PCI-required controls may not be applicable to other parts of the network.

Utilizing a third party to store, process, and transmit cardholder data or manage system components does not relieve a covered entity of its PCI compliance obligation. Unless the third-party service provider can demonstrate or provide evidence of PCI compliance, the service provider environment is considered to be an extension of the covered entity's cardholder data environment and is in scope.

What Is the PCI DDS Framework?

The PCI DSS framework includes stipulations regarding storage, transmission, and processing of payment card data, six core principles, required technical and operational security controls, testing requirements, and a certification process. Entities are required to validate their compliance. The number of transactions, the type of business, and the type of transactions determine specific validation requirements.

In today's Internet-based environment, there are multiple points of access to cardholder data and varying technologies. Version 3.0 is designed to accommodate the various environments where cardholder data is processed, stored, or transmitted—such as e-commerce, mobile acceptance, or cloud computing. Version 3.0 also recognizes that security is a shared responsibility and addresses the obligations of each business partner in the transaction chain.

In Practice

The Six PCI DSS Core Principles

The PCI DSS consists of six core principles, which are accompanied by 12 requirements. The six core principles are as follows:

- Build and maintain a secure network and systems.
- Protect cardholder data.
- Maintain a vulnerability management program.
- Implement strong access control measures.
- Regularly monitor and test networks.
- Maintain an information security policy.

Business-as-Usual Approach

PCI DSS version 3.0 emphasizes that compliance is not a point-in-time determination but rather an ongoing process. ***Business-as-usual*** is defined as the inclusion of PCI controls as part of an overall risk-based security strategy that is managed and monitored by the organization. According to the PCI Standards Council, a business-as-usual approach "enables an entity to monitor the effectiveness of their security controls on an ongoing basis, and maintain their PCI DSS compliant environment in between PCI DSS assessments." This means that organizations must monitor required controls to ensure they are operating effectively, respond quickly to control failures, incorporate PCI compliance impact assessments into the change-management process, and conduct periodic reviews to confirm that PCI requirements continue to be in place and that personnel are following secure processes.

Per the PCI Council, the version 3.0 updates are intended to do the following:

- Provide stronger focus on some of the greater risk areas in the threat environment.
- Build greater understanding of the intent of the requirements and how to apply them.
- Improve flexibility for all entities implementing, assessing, and building to the standards.
- Help manage evolving risks/threats.
- Align with changes in industry best practices.
- Eliminate redundant sub-requirements and consolidate policy documentation.

This approach mirrors best practices and reflects the reality that the majority of significant card breaches have occurred at organizations that were either self-certified or independently certified as PCI compliant.

What Are the PCI Requirements?

There are 12 top-level PCI requirements related to the six core principles. Within each requirement are sub-requirements and controls. The requirements are reflective of information security best practices. Quite often, the requirement's title is misleading in that it sounds simple but the sub-requirements and associated control expectations are actually quite extensive. The intent of and, in some cases, specific details of the requirements are summarized in the following sections. As you read them, you will notice that they parallel the security practices and principles we have discussed throughout this text.

In Practice

The 12 PCI DSS Top-Level Requirements

The PCI DSS consists of six core principles, which are accompanied by the following 12 requirements:

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and security parameters.
- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.
- Protect all systems against malware and regularly update antivirus software or programs.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need-to-know.
- Identify and authenticate access to system components.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security for all personnel.

Build and Maintain a Secure Network and Systems

The first core principle—build and maintain a secure network and systems—includes the following two requirements:

1. Install and maintain a firewall configuration to protect cardholder data.

   The basic objective of a firewall is ingress and egress filtering. The firewall does so by examining traffic and allowing or blocking transmissions based on a predefined rule set. The requirement extends beyond the need to have a firewall. It also addresses the following:

   - Identifying and documenting all connections
   - Designing a firewall architecture that protects cardholder data
   - Implementing consistent configuration standards
   - Documenting firewall configuration and rule sets
   - Having a formal change management process
   - Requiring rule-set business justification
   - Scheduling semiannual firewall rule-set review
   - Implementing firewall security controls such as anti-spoofing mechanisms

- Maintaining and monitoring firewall protection on mobile or employee-owned devices
- Publishing perimeter protection policies and related operational procedures

2. Do not use vendor-supplied defaults for system passwords and security parameters.

   Although this seems obvious, there may be default accounts, especially service accounts, that aren't evident or are overlooked. Additionally, systems or devices that are installed by third parties may be left at the default for ease of use. This requirement also extends far beyond its title and enters the realm of configuration management. Requirements include the following:

   - Maintaining an inventory of systems and system components
   - Changing vendor-supplied default passwords on all operating systems, applications, utilities, devices, and keys
   - Removing or disabling unnecessary default accounts, services, scripts, drivers, and protocols
   - Developing consistent configuration standards for all system components that are in accordance with industry-accepted system-hardening standards (such as ISO and NIST)
   - Segregating system functions based on security levels
   - Using secure technologies (for example, SFTP instead of FTP)
   - Encrypting all non-console administrative access
   - Publishing configuration management policies and related operational procedures

Protect Cardholder Data

The second core principle—Protect cardholder data—includes the following two requirements:

3. Protect stored card data.

   This is a very broad requirement. As mentioned earlier, the *cardholder data environment* is defined as the people, processes, and technology that handle cardholder data or sensitive authentication data. Sited protection mechanisms include encryption, truncation, masking and hashing, secure disposal, and secure destruction. Requirements include the following:

   - Data retention policies and practices that limit the retention of cardholder data and forbid storing sensitive authentication data post-authorization as well as card-verification code or value
   - Masking the PAN when displayed
   - Rendering the PAN unreadable anywhere it is stored
   - Protecting and managing encryption keys (including generation, storage, access, renewal, and replacement)

- Publishing data-disposal policies and related operational procedures
- Publishing data-handling standards that clearly delineate how cardholder data is to be handled
- Training for all personnel that interact with or are responsible for securing cardholder data

4. Encrypt transmission of cardholder data across open, public networks.

   The objective here is to ensure that data in transit over public networks cannot be compromised and exploited. An open and/or public network is defined as the Internet, wireless technologies including Bluetooth, cellular technologies, radio transmission, and satellite communications. The requirements include the following:

   - Using strong cryptography and security transmission protocols
   - Forbidding transmission of unprotected PANs by end-user messaging technologies such as email, chat, instant message, and text
   - Publishing transmission security policies and related operational procedures

Maintain a Vulnerability Management Program

The third core principle—Maintain a vulnerability management program—includes the following two requirements:

5. Protect all systems against malware and regularly update antivirus software or programs.

   As discussed in previous chapters, malware is a general term used to describe any kind of software or code specifically designed to exploit or disrupt a system or device, or the data it contains, without consent. Malware is one of the most vicious tools in the cybercriminal arsenal. The requirement includes:

   - Selecting an antivirus/anti-malware solution commensurate with the level of protection required
   - Selecting an antivirus/anti-malware solution that has the capacity to perform periodic scans and generate audit logs
   - Deploying the antivirus/anti-malware solution on all applicable in-scope systems and devices
   - Insuring that antivirus/anti-malware solutions are kept current
   - Insuring that antivirus/anti-malware solutions cannot be disabled or modified without management authorization
   - Publishing anti-malware security policies and related operational procedures
   - Training for all personnel on the implications of malware, disruption of the distribution channel, and incident reporting

6. Develop and maintain secure systems and architecture.

   This requirement mirrors the best practices guidance in Section 14 of ISO 27002:2013: Information Systems Acquisition, Development, and Maintenance, which focuses on the security requirements of information systems, applications, and code, from conception to destruction. The requirement includes the following:

   - Keeping up-to-date on new vulnerabilities
   - Assessing the risk of new vulnerabilities
   - Maintaining a patch management process
   - Adhering to security principles and best practices throughout the systems development lifecycle (SDLC)
   - Maintaining a comprehensive change management process, including back-out and restore procedures
   - Segregating the production environment from development, staging, and/or testing platforms
   - Adopting and internally publishing industry-accepted secure coding techniques (for example, OWASP)
   - Implementing code-testing procedures
   - Training developers in secure coding and vulnerability management practices
   - Publishing secure coding policies and related operational procedures

FYI: Focus on Malware Controls

Malware has been the tool of choice for some of the most significant data card breaches:

- November 2013: Criminals used malware to obtain unauthorized access to Target Corp's point-of-sale terminals, resulting in the compromise of 40 million credit and debit cards.
- January 2012: Criminals used an SQL injection attack to plant malware on the Global Payments, Inc.'s computer network and processing system, resulting in the compromise of 1.5 million credit and debit cards.
- July 2010: Criminals used an SQL injection attack to plant malware on the Euronet processing system, resulting in the compromise of 2 million credit and debit cards.
- January 2009: Criminals used malware to infiltrate the Heartland Payment Systems, resulting in the compromise of more than 130 million payment cards.
- November 2007: Criminals used malware to obtain unauthorized access to Hannaford Bros. Supermarkets' 271 store servers, resulting in the compromise of 4.2 million credit and debit cards.

Implement Strong Access Control Measures

The fourth core principle—Implement strong access control measures—includes the following three requirements:

7. Restrict access to cardholder data by business need-to-know.

   This requirement reflects the security best practices of deny all, need-to-know, and least privilege. The objective is to ensure that only authorized users, systems, and processes have access to cardholder data. The requirement includes the following:

   - Setting the default cardholder data access permissions to deny all
   - Identifying roles and system processes that need access to cardholder data
   - Determining the minimum level of access needed
   - Assigning permissions based on roles, job classification, or function
   - Reviewing permissions on a scheduled basis
   - Publishing access control policies and related operational procedures

8. Identify and authenticate access to system components.

   There are three primary objectives to this requirement. The first is to ensure that every user, system, and process is uniquely identified so that accountability is possible and to manage the account through its lifecycle. The second is to ensure that the strength of authentication credentials is commensurate with the access risk profile. The third is to secure the session from unauthorized access. This section is unique in that it sets specific implementation standards, including password length, password complexity, and session timeout. The requirement includes the following:

   - Assigning and requiring the use of unique IDs for each account (user or system) and process that accesses cardholder data and/or is responsible for managing the systems that process, transmit, or store cardholder data.
   - Implementing and maintaining a provisioning process that spans the account lifecycle from creation through termination. This includes access reviews and removing/disabling inactive user accounts at least every 90 days.
   - Allowing single-factor authentication for internal access if passwords meet the following minimum criteria: seven alphanumeric characters, 90-day expiration, and no reuse of the last four passwords. Account lockout mechanism's setting must lock out the user ID after six invalid login attempts and lock the account for a minimum of 30 minutes.
   - Requiring two-factor authentication for all remote network access sessions. Authentication mechanisms must be unique to each account.
   - Implementing session requirements, including a mandatory maximum 15-minute inactivity timeout that requires the user to reauthenticate, and monitoring remote vendor sessions.

- Restricting access to cardholder databases by type of account.
- Publishing authentication and session security policies and related operational procedures.
- Training users on authentication-related best practices, including how to create and manage passwords.

9. Restrict physical access to cardholder data.

   This requirement is focused on restricting physical access to media (paper and electronic), devices, and transmission lines that store, process, or transmit cardholder data. The requirement includes the following:

   - Implementing administrative, technical, and physical controls that restrict physical access to systems, devices, network jacks, and telecommunications lines within the scope of the cardholder environment.
   - Video monitoring physical access to sensitive areas, correlating with other entries, and maintaining evidence for a minimum of three months. The term ***sensitive areas*** refers to a data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.
   - Having procedures to identify and account for visitors.
   - Physically securing and maintaining control over the distribution and transport of any media that has cardholder data.
   - Securely and irretrievable destroying media (that has cardholder data) when it is no longer needed for business or legal reasons.
   - Protecting devices that capture card data from tampering, skimming, or substitution.
   - Training point-of-sale personnel about tampering techniques and how to report suspicious incidents.
   - Publishing physical security policies and related procedures.

FYI: Stealing Card Information Using a Skimmer

According to the Verizon 2013 Data Breach Investigations report, physical tampering accounts for 35% of data breaches; the common modus operandi being ATM and POS (point-of-sale) skimming. ***Skimming*** is theft of cardholder information by modifying a card swipe device and/or by attaching a card-reading device (aka, a skimmer) to a terminal or ATM. The prized target is debit cardholder data and PINs, which give the criminals the information they need to make counterfeit debit cards and withdraw cash from ATMs.

Skimming can be very lucrative. Before they were caught, a nine-month skimming operation in Oklahoma netted two men $400,000. According to their indictment, defendants Kevin Konstantinov and Elvin Alisuretove installed skimmers at Murphy's gas pumps in the parking lots of Walmart retail stores in Arkansas, Oklahoma, and Texas. They would leave the skimming devices in place for between one and two months. Then they'd collect the skimmers and use the stolen data to create counterfeit cards, visiting multiple ATMs throughout the region and withdrawing large amounts of cash.

Skimming devices are readily available online from dozens of stores for as little as $40. These devices are usually disguised under the name of "card reader" because they can also serve legitimate purposes. Several of the devices include built-in storage and wireless connectivity, which allow the criminals to transmit the stolen data. According to U.S. Secret Service Special Agent Cynthia Wofford, "Thieves travel to the U.S. for the very purpose of stealing credit and debit card data. The arrests we've made so far have led us to believe they're organized groups."

It is important that merchants learn how to inspect for and recognize skimming devices. "All About Skimmers," an excellent online primer (including pictures), is publicly available on the Krebs on Security site: http://krebsonsecurity.com/all-about-skimmers/.

Regularly Monitor and Test Networks

The fifth core principle—Regularly monitor and test networks—includes the following two requirements:

10. Track and monitor all access to network resources and cardholder data.

The nucleus of this requirement is the ability to log and analyze card data–related activity, with the dual objective of identifying precursors and indicators of compromise, and the availability of corroborative data if there is a suspicion of compromise. The requirement includes the following:

- Logging of all access to and activity related to cardholder data, systems, and supporting infrastructure. Logs must identity the user, type of event, date, time, status (success or failure), origin, and affected data or resource.
- Logging of user, administrator, and system account creation, modifications, and deletions.
- Ensuring the date and time stamps are accurate and synchronized across all audit logs.
- Securing audit logs so they cannot be deleted or modified.
- Limiting access to audit logs to individuals with a need to know.
- Analyzing audit logs in order to identify anomalies or suspicious activity.
- Retaining audit logs for at least one year, with a minimum of three months immediately available for analysis.
- Publishing audit log and monitoring policies and related operational procedures.

11. Regularly test security systems and processes.

    Applications and configuration vulnerabilities are identified on a daily basis. Ongoing vulnerability scans, penetration testing, and intrusion monitoring are necessary to detect vulnerabilities inherent in legacy systems and/or have been introduced by changes in the cardholder environment. The requirement to test security systems and processes is specific in how often testing must be conducted. This requirement includes the following:

    - Implementing processes to detect and identify authorized and unauthorized wireless access points on a quarterly basis.
    - Running internal and external network vulnerability scans at least quarterly and whenever there is a significant change in the environment. External scans must be performed by a PCI Approved Scanning Vendor (ASV).
    - Resolving all "high-risk" issues identified by the vulnerability scans. Verifying resolution by rescanning.
    - Performing annual network and application layer external and internal penetration tests using an industry-accepted testing approach and methodology (for example, NIST SP 800-115, OWASP). If issues are identified, they must be corrected and the testing redone to verify the correction.
    - Using intrusion detection (IDS) or intrusion prevention (IPS) techniques to detect or prevent intrusions into the network.
    - Deploying a change detection mechanism to alert personnel to unauthorized modifications of critical system files, configuration files, and content files.
    - Publishing security testing policies and related operational procedures.

Maintain an Information Security Policy

The sixth core principle—Maintain an information security policy—includes the final requirement:

12. Maintain a policy that addresses information security for all personnel.

    Of all the requirements, this may be the most inaptly named. A more appropriate title would be "Maintain a *comprehensive* information security program *(including whatever we've forgotten to include in the first 11 requirements)*." This requirement includes the following:

    - Establishing, publishing, maintaining, and disseminating an information security policy. The policy should include but not be limited to the areas noted in the other 11 PCI DSS requirements. The policy should be authorized by executive management or an equivalent body.
    - Annually reviewing, updating, and reauthorizing the information security policy.

- Implementing a risk assessment process that is based on an industry-accepted approach and methodology (for example, NIST 800-30, ISO 27005).
- Assigning responsibility for the information security program to a designated individual or team.
- Implementing a formal security awareness program.
- Educating personnel upon hire and then at least annually.
- Requiring users to annually acknowledge that they have read and understand security policies and procedures.
- Performing thorough background checks prior to hiring personnel who may be given access to cardholder data.
- Maintaining a vendor management program applicable to service providers with whom cardholder data is shared or who could affect the security of cardholder data.
- Requiring service providers to acknowledge in a written agreement their responsibility in protecting cardholder data.
- Establishing and practicing incident response capabilities.
- Establishing and practicing disaster response and recovery capabilities.
- Establishing and practicing business continuity capabilities.
- Annually testing incident response, disaster recovery, and business continuity plans and procedures.

In Practice

PCI Topic Summary and Chapter Cross Reference

Requirement	Topic	Chapter Cross-Reference
Install and maintain a firewall configuration to protect cardholder data.	Perimeter access controls	Ch. 9: Access Control Management
Do not use vendor-supplied defaults for system passwords and security parameters.	System inventory	Ch. 5: Asset Management
	System configuration	Ch. 8: Communications and Operations Security

Requirement	Topic	Chapter Cross-Reference
Protect stored cardholder data.	Data handling standards	Ch. 5: Asset Management
	Data retention standards	
	User training	Ch. 6: Human Resources Security
	Data and system disposal	Ch. 7: Physical and Environmental Security
	Key management	Ch. 10: Information Systems Acquisition, Development, and Maintenance
Encrypt transmission of cardholder data across open, public networks.	Encryption	Ch. 10: Information Systems Acquisition, Development, and Maintenance
	Secure transmission protocols	Ch. 8: Communications and Operations Security
Protect all systems against malware and regularly update antivirus software or programs.	Malware protection	Ch. 8: Communications and Operations Security
	User training	Ch. 6: Human Resources Security
Develop and maintain secure systems and applications.	Standard operating procedures	Ch. 8: Communications and Operations Security
	Patch management	
	Change management	
	Systems development lifecycle (SDLC)	Ch. 10: Information Systems Acquisition, Development, and Maintenance
	Secure coding procedures	
Restrict access to cardholder data by business need-to-know.	Security principles	Ch. 9: Access Control Management
	Role-based access control	
	Access reviews	
Identify and authenticate access to system components.	Authentication	Ch. 9: Access Control Management
	User provisioning	Ch. 6: Human Resources Security
	Session controls	Ch. 9: Access Control Management
	User training	Ch. 6: Human Resources Security

Requirement	Topic	Chapter Cross-Reference
Restrict physical access to cardholder data.	Physical access controls	Ch. 7: Physical and Environmental Security
	Data center monitoring	
	Media security	
	User training	Ch. 6: Human Resources Security
Track and monitor all access to network resources and cardholder data.	Audit log collection	Ch. 8: Communications and Operations Security
	Audit log analysis	
	Audit log management	
Regularly test security systems and processes.	Vulnerability scanning	Ch. 9: Access Control Management
	Penetration testing	
	Detection and alerting	Ch. 8: Communications and Operations Security
Maintain a policy that addresses information security for all personnel.	Security policy management	Ch. 4: Governance and Risk Management
	Risk assessment	
	Information security program management	
	Secure awareness program	Ch. 6: Human Resources Security
	Background checks	
	Acceptable use agreements	
	Vendor management program	Ch. 8: Communications and Operations Security
	Service provider contracts	
	Incident response capabilities	Ch. 11: Information Security Incident Management
	Disaster response and recovery capabilities	Ch. 12: Business Continuity Management

PCI Compliance

Complying with the PCI standards is a contractual obligation that applies to all entities involved in the payment card channel, including merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. The number of transactions, the type of business, and the type of transactions determine specific compliance requirements.

It is important to emphasize that PCI compliance is not a government regulation or law. The requirement to be PCI compliant is mandated by the payment card brands in order to accept card payments and/or be a part of the payment system. PCI standards augment but do not supersede legislative or regulatory requirements to protect personally identifiable information (PII) or other data elements.

Who Is Required to Comply with PCI DSS?

Merchants are required to comply with the PCI DSS. Traditionally a merchant is defined as a seller. It is important to note that the PCI DSS definition is a departure from the traditional definition. For the purposes of the PCI DSS, a merchant is defined as any entity that accepts American Express, Discover, JCB, MasterCard, or Visa payment cards as payment for goods and/or services (including donations). The definition does not use the terms *store*, *seller*, and *retail*; instead, the focus is on the payment side rather than the transaction type. Effectively, any company, organization, or individual that accepts card payments is a merchant. The mechanism for collecting data can be as varied as an iPhone-attached card reader, a parking meter, a point-of-sale checkout, or even an offline system.

Compliance Validation Categories

PCI compliance validation is composed of four levels, which are based on the number of transactions processed per year and whether those transactions are performed from a physical location or over the Internet. Each payment card brand has the option of modifying its requirements and definitions of PCI compliance validation levels. Given the dominance of the Visa brand, the Visa categorization is the one most often applicable. The Visa brand parameters for determining compliance validation levels are as follows. Any entity that has suffered a breach that resulted in an account data compromise may be escalated to a higher level.

- A Level 1 merchant meets one of the following criteria:
    - Processes over six million Visa payment card transactions annually (all channels).
    - A merchant that has been identified by any card association as a Level 1 merchant.
    - Any merchant that Visa, at its sole discretion, determines should meet the Level 1 requirements to minimize risk to the Visa system.
- A Level 2 entity is defined as any merchant—regardless of acceptance channel—processing one million to six million Visa transactions per year.

- A Level 3 merchant is defined as any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
- A Level 4 merchant is defined as any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants—regardless of acceptance channel—processing up to one million Visa transactions per year.

An annual onsite compliance assessment is required for Level 1 merchants. Level 2 and Level 3 merchants may submit a self-assessment questionnaire (SAQ). Compliance validation requirements for Level 4 merchants are set by the merchant bank. Submission of an SAQ is generally recommended but not required. All entities with externally facing IP addresses must engage an ASV to perform quarterly external vulnerability scans.

What Is a Data Security Compliance Assessment?

A ***compliance assessment*** is an annual onsite evaluation of compliance with the PCI DSS conducted by either a Qualified Security Assessor (QSA) or an Internal Security Assessor (ISA). The assessment methodology includes observation of system settings, processes, and actions, documentation reviews, interviews, and sampling. The culmination of the assessment is a Report on Compliance (ROC).

Assessment Process

The assessment process begins with documenting the PCI DSS cardholder environment and confirming the scope of the assessment. Generally, a QSA/ISA will initially conduct a GAP assessment to identify areas of noncompliance and provide remediation recommendations. Post-remediation, the QSA/ISA will conduct the assessment. In order to complete the process, the following must be submitted to either the acquiring financial institution or payment card brand:

- ROC completed by a QSA or ISA
- Evidence of passing vulnerability scans by an ASV
- Completion of the Attestation of Compliance by the assessed entity and the QSA
- Supporting documentation

FYI: What Are QSAs, ISAs, and ASVs?

The PCI Security Standards Council operates a number of programs to train, test, and certify organizations and individuals to assess and validate adherence to PCI Security Standards. These programs include QSA, ISA, and ASV.

Qualified Security Assessors (QSAs) are organizations that have been qualified by the PCI Council to have their employees assess compliance to the PCI DSS standard. QSAs are employees of these organizations who have been certified by the council to validate an entity's adherence to the PCI DSS.

Approved Scanning Vendors (ASVs) are organizations that validate adherence to certain DSS requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers.

Internal Security Assessors (ISAs) are sponsor companies that have been qualified by the council. The PCI SSC ISA Program consists of internal security audit professionals of sponsor organizations who are qualified through training from the council to improve their organization's understanding of the PCI DSS, facilitate the organization's interactions with QSAs, enhance the quality, reliability, and consistency of the organization's internal PCI DSS self-assessments, and support the consistent and proper application of PCI DSS measures and controls.

Source: PCI Security Standards Council (www.pcisecuritystandards.org/approved_companies_providers/)

Report on Compliance

As defined in the PCI DSS Requirements and Security Assessment Procedures, the ROC standard template includes the following sections:

- Section 1: Executive Summary
- Section 2: Description of Scope of Work and Approach Taken
- Section 3: Details about Reviewed Environment
- Section 4: Contact Information and Report Date
- Section 5: Quarterly Scan Results
- Section 6: Findings and Observations
- Compensating Controls Worksheets (if applicable)

Sections 1–5 provide a detailed overview of the assessed environment and establish the framework for the assessor's findings. The ROC template includes specific testing procedures for each PCI DSS requirement.

Section 6, "Findings and Observations," contains the assessor's findings for each requirement and testing procedure of the PCI DSS as well as information that supports and justifies each finding. The information provided in "Findings and Observations" summarizes how the testing procedures were performed and the findings achieved. This section includes all 12 PCI DSS requirements.

What Is the SAQ?

The SAQ is a validation tool for merchants that are not required to submit to an onsite data security assessment. There are two parts to the SAQ: the controls questionnaire and a self-certified attestation. Per the June 2012 PCI DSS SAQ Instructions and Guidelines, there are five SAQ categories. The categories and number of questions per assessment described next are based on PCI DSS V2 (as of November 2012, V3 SAQs were not yet available). The number of questions vary because the questionnaires are designed to be reflective of the specific payment card channel and the anticipated scope of the cardholder environment.

- **SAQ A** (13 questions) is applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format, and do not process or transmit any cardholder data on their systems or premises. This would never apply to face-to-face merchants.
- **SAQ P2PE** (18 questions) is applicable to merchants who process cardholder data only via payment terminals included in a validated and PCI SSC–listed Point-to-Point Encryption (P2PE) solution. This would never apply to e-commerce merchants. This category was added in June 2012.
- **SAQ B** (29 questions) is applicable to merchants who process cardholder data only via imprint machines or standalone, dial-out terminals. This would never apply to e-commerce merchants.
- **SAQ C-VT** (51 questions) is applicable to merchants who process cardholder data only via isolated virtual terminals on personal computers connected to the Internet. This would never apply to e-commerce merchants.
- **SAQ C** (80 questions) is applicable to merchants whose payment application systems are connected to the Internet either because the payment application system is on a personal computer that is connected to the Internet (for example, for email or web browsing) or the payment application system is connected to the Internet to transmit cardholder data.
- **SAQ D** (288 questions) is applicable to all other merchants not included in descriptions for SAQ types A through C as well as all service providers defined by a payment brand as eligible to complete an SAQ.

Completing the SAQ

In order to achieve compliance in question, the response to each question must either be “yes” or an explanation of a compensating control. ***Compensating controls*** are allowed when an organization cannot implement a specification but has sufficiently addressed the intent using an alternate method. If an entity cannot provide affirmative responses, it is still required to submit an SAQ.

To complete the validation process, the entity submits the SAQ and an accompanying Attestation of Compliance stating that it is or is not compliant with the PCI DSS. If the attestation indicates noncompliance, a target date for compliance along with an action plan needs to be provided. The attestation must be signed by an executive officer.

Are There Penalties for Noncompliance?

There are three types of fines: PCI noncompliance, Account Data Compromise Recovery (ADCR) for compromised domestic-issued cards, and Data Compromise Recovery Solution (DCRS) for compromised international-issued cards. Noncompliance penalties are discretionary and can vary greatly, depending on the circumstances. They are not openly discussed or publicized.

FYI: 2012 Global Payments PCI Breach Cost $95.9 Million

Global Payments, an Atlanta-based payments processor, disclosed a data breach in March 2012. According to the company, affected were an estimated 1.5 million payment cards as well as personal information collected from merchants who applied for processing services. Industry analysts believe more than seven million card accounts may have been compromised.

The payment brands decertified Global Payments and removed it from the list of PCI-compliant service providers. As of October 2013, Global Payments successfully completed ROCs covering all systems that process, store, transmit, or otherwise utilize card data and were returned to the network list of PCI-compliant service providers. In its quarterly earnings reports (SEC 10-Q), Global Payments outlined the costs related to the data breach. The numbers include an anticipated insurance recovery offset of $28 million dollars.

- $60 million for professional fees and other costs associated with the investigation and remediation, incentive payments to certain business partners, and costs associated with credit monitoring and identity protection insurance.
- $35.9 million for the total of estimated fraud losses, fines, and other charges that will be imposed by the card networks.

Fines and Penalties

More financially significant than PCI noncompliance fines, a data compromise could result in ADCR and/or DCRS penalties. Due to the structure of the payment system, if there is a merchant compromise, the payment brands impose the penalties on the bank that issued the account. The banks pass all liability downstream to the entity. The fines may be up to $500,000 per incident. In addition, the entity may be liable for the following:

- All fraud losses perpetrated using the account numbers associated with the compromise (from date of compromise forward)
- Cost of reissuance of cards associated with the compromise (approximately $50 per card)
- Any additional fraud prevention/detection costs incurred by credit card issuers associated with the compromise (that is, additional monitoring of system for fraudulent activity)
- Increased transaction fees

At their discretion, the brands may designate any size compromised merchants as Level 1, which requires an annual onsite compliance assessment. Acquiring banks may choose to terminate the relationship.

Alternately, the payment brands may waive fines in the event of a data compromise if there is no evidence of noncompliance with PCI DSS and brand rules. According to Visa, "to prevent fines, a merchant must maintain full compliance at all times, including at the time of breach as demonstrated during a forensic investigation. Additionally, a merchant must demonstrate that prior to the compromise, the compromised entity had already met the compliance validation requirements, demonstrating full compliance." This is an impossibly high standard to meet. In reality, uniformly when there has been a breach, the brands have declared the merchant to be noncompliant.

FYI: Genesco v. Visa for Recovery of PCI Fines

Filed in March 2013 in Nashville District Court, Genesco v. Visa is the first direct lawsuit against a credit card company for the levying of PCI fines. Genesco, a Tennessee corporation, is a specialty retailer that sells footwear, headwear, sports apparel, and accessories in more than 2,440 retail stores in the U.S., Canada, U.K., and the Republic of Ireland as well as on an Internet website.

Genesco brought suit against Visa to recover $13,298,900.16 in noncompliance fines and issuer reimbursement fees that Visa imposed. The fines assessed stemmed from the December 2010 breach of Genesco's payment processing network due to a criminal cyber attack. Genesco claims in its complaint that Visa had no reasonable basis for concluding that it was noncompliant with the PCI standards, and that there was no actual theft of cardholder data for the accounts in question. Genesco's complaint brings claims for breach of contract and violation of the California Unfair Business Practices Act as well as related claims.

The case is in its early stages. The outcome is being closely watched as legal experts contend that a ruling in favor of Genesco could undermine the credit card companies' ability to assess PCI fines.

Summary

The Payment Card Industry Data Security Standard, known as PCI DSS, applies to all entities involved in the payment card channel, including merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. The PCI DSS framework includes stipulations regarding storage, transmission, and processing of payment card data, six core principles, 12 categories of required technical and operational security controls, testing requirements, and a validation and certification process. Entities are required to validate their compliance. The number of transactions, the type of business, and the type of transactions determine specific validation requirements.

Compliance with PCI DSS is a payment card channel contractual obligation. It is not a government regulation or law. The requirement to be PCI compliant is mandated by the payment card brands in order to accept card payments and/or be part of the payment system. PCI standards augment but do not supersede legislative or regulatory requirements to protect PII or other data elements.

Overall, the PCI DSS requirements are reflective of information security best practices. Version 3.0 introduced a risk model designed to allow entities to respond quickly to emerging criminal threats to the payment channel.

Test Your Skills

MULTIPLE CHOICE QUESTIONS

1. The majority of payment card fraud is borne by __________.

   A. consumers

   B. banks, merchants, and card processors

   C. Visa and MasterCard

   D. All of the above

2. Which of the following statements best describes the objective of the PCI Security Standards Council?

   A. The objective of the PCI Security Standards Council is to create a single enforcement body.

   B. The objective of the PCI Security Standards Council is to create a common penalty structure.

   C. The objective of the PCI Security Standards Council is to create a single payment card security standard.

   D. The objective of the PCI Security Standards Council is to consolidate all payment card rules and regulations.

3. A skimmer can be used to read ____________.
   - A. the cardholder data
   - B. sensitive authentication data
   - C. the associated PIN
   - D. All of the above

4. According to PCI DDS, which of the following is true of the primary account number (PAN)?
   - A. It must never be stored.
   - B. It can only be stored in an unreadable (encrypted) format.
   - C. It should be indexed.
   - D. It can be stored in plain text.

5. Which of the following statements best describes sensitive authentication data?
   - A. Sensitive authentication data must never be stored, ever.
   - B. Sensitive authentication data can be stored indefinitely in an unreadable (encrypted) format.
   - C. Sensitive authentication data should be masked.
   - D. Sensitive authentication data may never be stored post-authorization.

6. Which of the following tasks is the PCI Security Standards Council *not* responsible for?
   - A. Creating a standard framework
   - B. Certifying ASVs and QSAs
   - C. Providing training and educational materials
   - D. Enforcing PCI compliance

7. Which of the following statements best describes PCI DSS Version 3?
   - A. PCI DSS Version 3 is a departure from earlier versions because the core principles have changed.
   - B. PCI DSS Version 3 is a departure from earlier versions because it promotes a risk-based approach.
   - C. PC I DSS Version 3 is a departure from earlier versions because the penalties have increased.
   - D. PC I DSS Version 3 is a departure from earlier versions because it shifts the compliance obligation to service providers.

8. Which of the following statements best describes the “cardholder data environment”?

   A. The “cardholder data environment” includes the people that handle cardholder data or sensitive authentication data.

   B. The “cardholder data environment” includes the processes that handle cardholder data or sensitive authentication data.

   C. The “cardholder data environment” includes the technology that handles cardholder data or sensitive authentication data.

   D. All of the above.

9. Sensitive authentication data does *not* include which of the following?

   A. PINs

   B. Card expiration date

   C. CVV2

   D. Mag stripe or chip data

10. Which of the following statements best describes the PAN?

    A. If the PAN is not stored, processed, or transmitted, then PCI DSS requirements do not apply.

    B. If the PAN is not stored, processed, or transmitted, then PCI DSS requirements apply only to e-commerce merchants.

    C. If the PAN is not stored, processed, or transmitted, then PCI DSS requirements apply only to Level 1 merchants.

    D. None of the above.

11. Which of the following statements is true?

    A. When a debit or ATM card is lost or stolen, the cardholder liability is limited to $50.

    B. When a debit or ATM card is lost or stolen, the cardholder is responsible for all charges.

    C. When a debit or ATM card is lost or stolen, the cardholder liability depends on when the loss or theft is reported.

    D. When a debit or ATM card is lost or stolen, the cardholder is never responsible for the charges.

12. The terms CVV2, CID, CVC2, and CVV2 all refer to the ___________.

    A. authentication data

    B. security code

    C. expiration date

    D. account number

13. There are 12 categories of PCI standards. In order to be considered compliant, an entity must comply with or document compensating controls for _________.

- **A.** All of the requirements
- **B.** 90% of the requirements
- **C.** 80% of the requirements
- **D.** 70% of the requirements

14. Which of the following is *not* considered a basic firewall function?

- **A.** Ingress filtering
- **B.** Packet encryption
- **C.** Egress filtering
- **D.** Perimeter protection

15. Which of the following is considered a secure transmission technology?

- **A.** FTP
- **B.** HTTP
- **C.** Telnet
- **D.** SFTP

16. Which of the following statements best describes key management?

- **A.** Key management refers to the generation, storage, and protection of encryption keys.
- **B.** Key management refers to the generation, storage, and protection of server room keys.
- **C.** Key management refers to the generation, storage, and protection of access control list keys.
- **D.** Key management refers to the generation, storage, and protection of card manufacturing keys.

17. Which of the following methods is an acceptable manner in which a merchant can transmit a PAN?

- **A.** Using cellular texting
- **B.** Using an HTTPS/SSL session
- **C.** Using instant messaging
- **D.** Using email

18. Which of the following statements is true?

    A. The PCI requirement to protect all systems against malware requires that merchants select a malware solution commensurate with the level of protection required.

    B. The PCI requirement to protect all systems against malware requires that merchants select a PCI-certified anti-malware solution.

    C. The PCI requirement to protect all systems against malware requires that merchants select a PCI-compliant anti-malware solution.

    D. The PCI requirement to protect all systems against malware requires that merchants select a malware solution that can be disabled if necessary.

19. Which of the following documents lists injection flaws, broken authentication, and cross-site scripting as the top three application security flaws?

    A. ISACA Top Ten

    B. NIST Top Ten

    C. OWASP Top Ten

    D. ISO Top Ten

20. Which of the following security principles is best described as the assigning of the minimum required permissions?

    A. Need-to-know

    B. Deny all

    C. Least privilege

    D. Separation of duties

21. Which of the following is an example of two-factor authentication?

    A. Username and password

    B. Password and challenge question

    C. Username and token

    D. Token and PIN

22. Skimmers can be installed and used to read cardholder data enter at ________.

    A. point-of-sale systems

    B. ATMs

    C. gas pumps

    D. All of the above

23. Which of the following best describes log data?

- **A.** Log data can be used to identify indicators of compromise.
- **B.** Log data can be used to identify primary account numbers.
- **C.** Log data can be used to identify sensitive authentication data.
- **D.** Log data can be used to identify cardholder location.

24. Quarterly external network scans must be performed by a __________.

- **A.** managed service provider
- **B.** Authorized Scanning Vendor
- **C.** Qualified Security Assessor
- **D.** independent third party

25. In keeping with the best practices set forth by the PCI standard, how often should information security policies be reviewed, updated, and authorized?

- **A.** Once
- **B.** Semi-annually
- **C.** Annually
- **D.** Bi-annually

26. Which of the following is true of PCI requirements?

- **A.** PCI requirements augment regulatory requirements.
- **B.** PCI requirements supersede regulatory requirements.
- **C.** PCI requirements invalidate regulatory requirements.
- **D.** None of the above.

27. The difference between a Level 1 merchant and Levels 2–4 merchants is that _____________ ________________________________.

- **A.** Level 1 merchants must have 100% compliance with PCI standards.
- **B.** Level 1 merchants must complete an annual onsite compliance assessment.
- **C.** Level 1 merchants must have quarterly external vulnerabilities scans.
- **D.** Level 1 merchants must complete a self-assessment questionnaire.

28. Which of the following statements is true of entities that experience a cardholder data breach?

- **A.** They must pay a minimum $50,000 fine.
- **B.** They may be reassigned as a Level 1 merchant.
- **C.** They will no longer be permitted to process credit cards.
- **D.** They must report the breach to a federal regulatory agency.

29. Which of the following statements best describes the reason different versions of the SAQ are necessary?

    A. The number of questions vary by payment card channel and scope of environment.

    B. The number of questions vary by geographic location.

    C. The number of questions vary by card brand.

    D. The number of questions vary by dollar value of transactions.

30. Which of the following statements is true of an entity that determines it is not compliant?

    A. The entity does not need to submit an SAQ.

    B. The entity should notify customers.

    C. The entity should submit an action plan along with its SAQ.

    D. The entity should do nothing.

EXERCISES

EXERCISE 15.1: Understanding PCI DSS Obligations

1. Compliance with PCI DSS is a contractual obligation. Explain how this differs from a regulatory obligation.
2. Which takes precedence—a regulatory requirement or a contractual obligation? Explain your answer.
3. Who enforces PCI compliance? How is it enforced?

EXERCISE 15.2: Understanding Cardholder Liabilities

1. What should a consumer do if he or she misplaces a debit card? Why?
2. Go online to your bank's website. Does it post instructions on how to report a lost or stolen debit or credit card? If yes, summarize their instructions. If no, call the bank and request the information be sent to you. (If you don't have a bank account, choose a local financial institution.)
3. Explain the difference between the Fair Credit Billing Act (FCBA) and the Electronic Fund Transfer Act (EFTA).

EXERCISE 15.3: Choosing an Authorized Scanning Vendor

1. PCI security scans are required for all merchants and service providers with Internet-facing IP addresses. Go online and locate three PCI Council Authorized Scanning Vendors (ASV) that offer quarterly PCI security scans.
2. Read their service descriptions. What are the similarities and differences?
3. Recommend one of the ASVs. Explain your reasoning.

EXERCISE 15.4: Understanding PIN and Chip Technologies

1. Payment cards issued in the United States store sensitive authentication information in the magnetic stripe. What are the issues associated with this configuration?
2. Payment cards issued in Europe store sensitive authentication information in an embedded microchip. What is the advantage of this configuration?
3. Certain U.S. financial institutions will provide a chip-embedded card upon request. Identify at least one card issuer who will do so. Does it charge extra for the card?

EXERCISE 15.5: Identifying Merchant Compliance Validation Requirements

Complete the following table:

Merchant Level	Criteria	Validation Requirement
	Processes fewer than 20,000 e-commerce transactions annually	
Level 2		
		Required onsite annual audit

PROJECTS

PROJECT 15.1: Applying Encryption Standards

Encryption is referenced a number of times in the PCI DSS standard. For each of the PCI requirements listed below:

1. Explain the rationale for the requirement.
2. Identify a encryption technology that can be used to satisfy the requirement.
3. Identify a commercial application that can be used to satisfy the requirement.

    - PCI DSS V3. 3.4.1—If disk encryption is used, logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials).
    - PCI DSS V3. 4.1—Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.
    - PCI DSS V3. 4.1.1—Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, and use industry best practices to implement strong encryption for authentication and transmission.

PROJECT 15.2: Completing an SAQ

All Level 2 and Level 3 merchants and some Level 4 merchants are required to submit a Self-Assessment Questionnaire (SAQ). Access the Official PCI Security Standards Council website and download SAQ A and SAQ C.

1. What are the differences and similarities between SAQ A and C? Describe the merchant environment for each SAQ.
2. Explain how the scope of a cardholder environment impacts the completion of SAQ C. Give two specific examples where narrowing the scope would be beneficial.
3. Read the SAQ C compensating controls section. Explain what is meant by compensating controls and give two specific examples.

PROJECT 15.3: Reporting an Incident

Assume you are a Level 2 merchant and your organization suspects a breach of Visa cardholder information.

1. Go to http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html. Document the steps you should take.
2. Does your state have a breach notification law? If so, would you be required to report this type of breach to a state authority? Would you be required to notify customers? What would you need to do if you had customers who lived in a neighboring state?
3. Have there been any major card breaches within the last 12 months that affected residents of your state? Summarize such an event.

Case Study

Payment Card Data Breaches

Target Corp., a major retailer in the United States, disclosed a breach in December 2013. Global Payments, an Atlanta-based payments processor, disclosed a data breach in March 2012.

Research both events and answer the following questions:

A. Target Corp.

1. What are the dates of the incident?
2. Who first reported the breach?
3. What information was compromised?
4. How many cardholders were affected?
5. How did Target notify cardholders?

6. Is there any indication of how the data was acquired?
7. Is there any evidence that the criminals used the card data?

B. Global Payments

1. Who first reported the incident?
2. What are the dates associated with the compromise?
3. What information was compromised?
4. How many cardholders were affected?
5. Is there any indication of how the data was acquired?
6. Were losses sustained by any organization other than Global Payments?
7. What type of notification was required?

C. Prior to the breach, Global Payments was a certified Level 1 PCI-compliant organization. Due to the breach, Global Payments was decertified and required to undergo a rigorous recertification process. Should a card data compromise be a trigger for decertification? Why or why not?

References

"Cash Dying as Credit Card Payments Predicted to Grow in Volume," *Huffington Post*, June 6, 2012, accessed 10/2013, www.huffingtonpost.com/2012/06/07/credit-card-payments-growth_n_1575417.html.

"2013 Data Breach Investigations Report," Verizon, accessed 11/2013, www.verizonenterprise.com/DBIR/2013.

"Data Security—PCI Mandatory Compliance Programs," Wells Fargo, accessed 11/2013, www.wellfargo.com/biz/merchant/service/manage/risk/security.

"Debit and Credit Card Skimming," Privacy Sense, accessed 11/2013, www.privacysense.net/debit-and-credit-card-skimming/.

"Genesco, Inc. v. VISA U.S.A., Inc., VISA Inc., and VISA International Service Association," United States District Court for the Middle District of Tennessee, Nashville Division. Filed March 7, 2013, Case 3:13-cv-00202.

"Global Payments Breach Tab: $94 Million," Bank InfoSecurity, accessed 11/2013, www.bankinfosecurity.com/global-payments-breach-tab-94-million-a-5415/op-1.

Green, Joe. "Credit card 'skimming' a real danger, Secret Service officials warn," *South NJ Times*, accessed 11/2013, www.nj.com/gloucester-county/index.ssf/2013/10/creditdebit_card_skimming_a_real_danger_south_jersey_secret_service_officials_warn.html.

"Global Payments Sec 10-Q Filing," Investor Relations, accessed 11/2013, http://investors.globalpaymentsinc.com/financials.cfm.

Krebs, Brian. "All about Skimmers," accessed 11/2013, http://krebsonsecurity.com/all-about-skimmers/.

"Lost or Stolen Cred, ATM and Debit Cards," Federal Trade Commission Consumer Information, accessed 11/2013, www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

"Merchant PCI DSS Compliance," Visa, accessed 11/2013, http://usa.visa.com/merchants/risk_management/cisp_merchants.html.

"Payment Card Industry Data Security Standard, Navigating PCI DSS, Understanding the Intent of the Requirements, Version 2.0," PCI Security Standards Council, LLC, October 2010.

"Payment Card Industry Data Security Standard, PCI DSS Quick Reference Guide, Understanding the Payment Card Industry Data Security Standard, Version 2.0," PCI Security Standards Council LLC, October 2010.

"Payment Card Industry Data Security Standard, ROC Reporting Instructions for PCI DSS 2.0," PCI Security Standards Council, LLC, September 2011.

"Payment Card Industry Data Security Standard, Self-Assessment Questionnaire Instructions and Guidelines, Version 2.1," PCI Security Standards Council, LLC, June 2012.

"Payment Card Industry Data Security Standard and Payment Application Data Security Standard, Version 3.0: Change Highlights," PCI Security Standards Council, LLC, August 2013.

"Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, Version 3.0," PCI Security Standards Council, LLC, November 2013.

"Plastic, Please! The Dominance of Card Payments," True Merchant, accessed 10/2013, www.true-merchant.com/plastic-please-the-dominance-of-card-payments/.

"Processor Global Payments Prepares to Close the Book on Its Data Breach," Digital Transactions, accessed 11/2013, http://digitaltransactions.net/news/story/3940.

United States of America v. Kevin Konstantinov and Elvin Alisuretove, United States District Court for the Eastern District of Oklahoma. Filed July 9, 2013, Case CR13-062-RAW.

United States of America v. Drinkman, Kalinin, Kotov, Rytikov, Smilianets, United States District Court, District of New Jersey, Indictment case number 09-626(JBS) (8-2).

Appendix A

Information Security Program Resources

National Institute of Standards and Technology (NIST) Special Publications

http://csrc.nist.gov/publications/PubsSPs.html

- SP 800-12: An Introduction to Computer Security: The NIST Handbook
- SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
- SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model
- SP 800-23: Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- SP 800-30: Risk Management Guide for Information Technology Systems
- SP 800-34: Contingency Planning Guide for Information Technology System, Revision 1
- SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View
- SP 800-40: Creating a Patch and Vulnerability Management Program
- SP 800-41: Guidelines on Firewalls and Firewall Policy

- SP 800-42: Guidelines on Network Security Testing
- SP 800-45: Guidelines on Electronic Mail Security
- SP 800-46: Guide to Enterprise Telework and Remote Access Security
- SP 800-50: Building an Information Technology Security Awareness and Training Program
- SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations
- SP 800-57: Recommendations for Key Management—Part 1: General (Revision 3)
- SP 800-57: Recommendations for Key Management—Part 2: Best Practices for Key Management Organization
- SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories (Two Volumes)
- SP 800-61: Computer Security Incident Handling Guide
- SP 800-64: Security Considerations in the System Development Life Cycle
- SP 800-66: Guide to Integrating Forensic Techniques into Incident Response
- SP 800-77: Guide to IPsec VPNs
- SP 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- SP 800-84: Guide to Test, Training, and Exercise Programs for Information Technology Plans and Capabilities
- SP 800-88: Guidelines for Media Sanitization
- SP 800-92: Guide to Computer Security Log Management
- SP 800-94: Guide to Intrusion Detection and Prevention Systems
- SP 800-100: Information Security Handbook: A Guide for Managers
- SP 800-111: Guide to Storage Encryption Technologies for End User Devices
- SP 800-113: Guide to SSL VPNs
- SP 880-114: User’s Guide to Securing External Devices for Telework and Remote Access
- SP 800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)

Federal Financial Institutions Examination Council (FFIEC) IT Handbooks

http://ithandbook.ffiec.gov/it-booklets.aspx

- Business Continuity Planning
- Development and Acquisition
- Information Security
- (Risk) Management
- Outsourcing Technology Services
- Supervision of Technology Service Providers (TSP)

Department of Health and Human Services HIPAA Security Series

www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

1. Security 101 for Covered Entities
2. Security Standards, Administrative Safeguards
3. Security Standards, Physical Safeguards
4. Security Standards, Technical Safeguards
5. Security Standards: Organizational, Policies, and Procedures and Documentation Requirements
6. Basics of Risk Analysis and Risk Management
7. Security Standards: Implementation for the Small Provider

Payment Security Standards Council Documents Library

https://www.pcisecuritystandards.org/security_standards/documents.php

- PCI DSS v3.0
- PCI DSS Summary of Changes v2.0 to v3.0
- PCI DSS Quick Start Guide

Information Security Professional Development and Certification Organizations

- International Information Systems Security Certification Consortium (ISC2): www.isc2.org
- Information Systems Audit and Control Association (ISACA): www.isaca.org
- Information Systems Security Association, Inc. (ISSA): www.issa.org
- SANS Institute: www.sans.org
- Disaster Recovery Institute (DRI): www.drii.org
- The Institute of Internal Auditors: www.theiia.org

Appendix B

Sample Information Security Policy

Introduction

The objective of our Information Security Policy is to protect and respect the confidentiality, integrity, and availability (CIA) of client information, company proprietary data and employee data as well as the infrastructure that supports our services and business activities. Our Information Security Policy has been designed to meet or exceed applicable federal and state information security-related regulations contractual obligations.

The scope of the Information Security Policy extends to all functional areas and all employees, Directors, consultants, contractors, temporary staff, co-op students, interns, partners and third-party employees, and joint venture partners unless explicitly excluded. At first glance, the policy may appear daunting. If you take a look at the Table of Contents, you will see that the Information Security Policy is organized by category. These categories form the framework of our Information Security Program. Supporting the policies are implementation standards, guidelines, and procedures. You can find these documents in the Governance section of our online company library.

Diligent information security practices are a civic responsibility and a team effort involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee and affiliate to know, understand, and adhere to these policies, and to conduct their activities accordingly. If you have any questions or would like more information, I encourage you to contact either our Compliance Officer or Chief Information Security Officer (CISO).

I thank you in advance for your support as we all do our best to create a secure environment and to fulfill our mission. – <<Name, Title, Date>>

Policy Exemptions

Where compliance is not technically feasible or justified by business needs, an exemption may be granted. Exemption requests must be submitted in writing to the Chief Operating Officer (COO) including justification and benefits attributed to the exemption. Unless otherwise stated, the COO and the Chief Executive Officer (CEO) have the authority to grant waivers.

Policy Violation

Wilful violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. Additionally, individuals may be subject to civil and criminal prosecution.

Version Control

Revision	Originator	Change Date	Change Description	Approver Name	Approved Date

Section 1: Governance and Risk Management

Overview

Governance is the set of responsibilities and practices exercised by management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly. The principal objective of an organization's risk management process is to provide those in leadership and data steward roles with the information required to make well-informed decisions.

Goals and Objectives for Section 1: Governance and Risk Management

- To demonstrate the organizational commitment to implementing and maintaining an Information Security Policy and supporting structure.
- To ensure that management is actively engaged in the success of the Information Security Policy and Program.
- To provide the support and oversight required to maintain an effective policy and program.
- To define organizational roles and responsibilities.
- To provide the framework for effective risk management and continuous assessment.

Governance and Risk Management Policy Index

1.1. Information Security Policy

1.2. Information Security Policy Authorization and Oversight

1.3. Chief Information Security Officer (CISO)

1.4. Information Security Steering Committee

1.5. Information Security Risk Management Oversight

1.6. Information Security Risk Assessment

1.7. Information Security Risk Response

1.0 Governance and Risk Management Policy

1.1. Information Security Policy

1.1.1. The company is required to have a written Information Security Policy and supporting documents.

1.1.2. Executive Management is responsible for establishing the mandate and general objectives of the aggregate Information Security Policy.

1.1.3. Information security policies must support organizational objectives.

1.1.4. Information security policies must comply with relevant statutory, regulatory, and contractual requirements.

1.1.5. Information security policies must be communicated to all relevant parties both within and external to the company.

1.1.6. As applicable, standards, guidelines, plans, and procedures must be developed to support the implementation of Information Security Policy objectives and requirements.

1.1.7. For the purpose of educating the workforce, user-level documents will be derived from the Information Security Policy including but not limited to acceptable use and agreement, and information handling instructions.

1.1.8. Any Information Security Policy distributed outside the organization must be sanitized.

1.1.9. All documentation will be retained for a period of six years from the last effective date.

1.2. Information Security Policy Authorization and Oversight

1.2.1. The Board of Directors must authorize the Information Security Policy.

1.2.2. An annual review of the Information Security Policy must be conducted.

1.2.2.1. The CISO is responsible for managing the review process.

1.2.3. Changes to the policy must be presented to and approved by a majority of the Board of Directors.

1.2.4. The COO and the CISO will jointly present an annual report to the Board of Directors that provides them the information necessary to measure the organizations' adherence to the Information Security Policy objectives and the maturity of the Information Security Program.

1.2.5. When in-house knowledge is not sufficient to review or audit aspects of the Information Security Policy, or if circumstances dictate independence, third-party professionals must be engaged.

1.3. Chief Information Security Officer (CISO)

1.3.1. The COO will appoint the CISO.

1.3.2. The CISO will report directly to the COO.

1.3.3. At his/her discretion, the CISO may communicate directly with members of the Board of Directors.

1.3.4. The CISO is responsible for managing the Information Security Program, assuring compliance with applicable regulations and contractual obligations, and working with business units to align information security requirements and business initiatives.

1.3.5. The CISO will function as an internal consulting resource on information security issues.

1.3.6. The CISO will chair the Information Security Steering Committee.

1.3.7. The CISO will be a standing member of the Incident Response Team and the Continuity of Operations Team.

1.3.8. Quarterly, the CISO will report to the Executive Management Team on the overall status of the Information Security Program. The report should discuss material matters including such issues as risk assessment, risk management, and control decisions, service provider arrangements, results of testing, security breaches or violations, and recommendations for policy changes.

1.4. Information Security Steering Committee

1.4.1. The Information Security Steering Committee serves in an advisory capacity in regard to the implementation, support, and management of the Information Security Program, alignment with business objectives, and compliance with all applicable state and federal laws and regulations.

1.4.2. The Information Security Steering Committee provides an open forum to discuss business initiatives and security requirements. Security is expected to be given the same level of respect as other fundamental drivers and influencing elements of the business.

1.4.3. Standing membership shall include the CISO (chair), the COO, the Director of Information Technology, the Risk Officer, the Compliance Officer, and business unit representatives. Adjunct committee members may include but are not limited to representatives of human resources, training, and marketing.

1.4.4. The Information Security Steering Committee will meet on a monthly basis.

1.5. Information Security Risk Management Oversight

1.5.1. Executive Management in consultation with the Board of Directors is responsible for determining the organizational risk appetite and risk tolerance levels.

1.5.2. Executive Management will communicate the above to decision makers throughout the company.

1.5.3. The CISO in consultation with the Chief Risk Officer is responsible for determining the information security risk assessment schedule, managing the risk assessment process, certifying results, jointly preparing risk reduction recommendations with business process owners, and presenting the results to Executive Management.

1.5.4. The Board of Directors will be apprised by the COO of risks that endanger the organization, stakeholders, employees, or customers.

1.6. Information Security Risk Assessment

1.6.1. The company must adopt an information security risk assessment methodology to ensure consistent, repeatable, and comparable results.

1.6.2. Information security risk assessments must have a clearly defined and limited scope. Assessments with a broad scope become difficult and unwieldy in both their execution and the documentation of the results.

1.6.3. The CISO is charged with developing an information security risk assessment schedule based upon the information systems criticality and information classification level.

1.6.4. In addition to scheduled assessments, information security risk assessments must be conducted prior to the implementation of any significant change in technology, process, or third-party agreement.

1.6.5. The CISO and the business process owner are jointly required to respond to risk assessment results and develop risk reduction strategies and recommendations.

1.6.6. Risk assessment results and recommendations must be presented to Executive management.

1.7. Information Security Risk Response

1.7.1. The initial results of all risk assessments must be provided to Executive Management and the business process owner within seven days of completion.

1.7.2. Low level risks can be accepted by the business process owner.

1.7.3. Elevated risks and severe risks (or comparable rating) must be responded to within 30 days. Response is the joint responsibility of the business process owner and the CISO.

1.7.3.1. Risk reduction recommendations can include risk acceptance, risk mitigation, risk transfer, risk avoidance, or a combination thereof.

1.7.3.2. Recommendations must be documented and include a applicable level of detail.

1.7.4. Elevated and severe risks can be accepted by Executive Management.

1.7.5. The Board of Directors must be informed of accepted severe risk. At their discretion, they can choose to overrule acceptance.

Supporting Resources and Source Material

- ISO 27002:2013 Section 5 Information Security Policy
- ISO 27002:2013 Section 6 Organization of Information Security
- ISO 27005:2005 Risk Management
- NIST SP 800-30 Risk Management Guide for Information Technology Systems
- NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Section 2: Asset Management

Overview

Asset management in the context of information security is the identification and categorization of information based upon predefined criteria which generally includes confidentiality, contractual, and regulatory requirements. Classification levels are then used to define the control environment including handling and labeling standards.

Goals and Objectives for Section 2: Asset Management

- To assign specific responsibilities to data stewards and data custodians.
- To establish data classification levels.
- To ensure that the company maintains an inventory of information security assets
- To ensure that appropriate handling standards are developed for each classification.

Asset Management Policy Index

2.0 Asset Management Policy

2.1. Information Ownership

2.1.1. All information assets and systems must have an assigned owner.

2.1.2. The Office of Information Security will maintain an inventory of information asset ownership.

2.1.3. Owners are required to classify information and information systems in accordance with the organizational classification guidelines.

2.1.4. Owners are responsible for determining the required level of protection.

2.1.5. Owners must authorize internal information and information system access rights and permissions.

2.1.6. Owners must review and reauthorize access rights and permissions on an annual basis.

2.1.7. Owners must authorize third-party access to information or information systems. This includes information provided to a third party.

2.1.8. Implementation and maintenance of controls is the responsibility of the Office of Information Security; however, accountability will remain with the owner of the asset.

2.2. Information Classification Policy

2.2.1. The company will use a four-tiered data classification schema consisting of protected, confidential, restricted, and public.

2.2.2. The company will publish definitions for each classification.

2.2.3. The criteria for each level will be maintained by and available from the Office of Information Security.

2.2.4. All information will be associated with one of the four data classifications. It is the responsibility of information owners to classify data.

2.2.5. Information systems containing information from multiple classification levels shall be secured in accordance with the requirements of the highest classification level.

2.2.6. Data classification will remain in force regardless of the location or state of the data at any given time. This includes backup and archive media and locations.

2.2.7. The classification system will allow that classifications of information assets may change over time.

2.2.8. Each classification shall have documented handling requirements.

2.3. Information Classification Handling and Labeling Requirements

2.3.1. Each classification of data will have documented handling standards for the following categories: storage, transmission, communication, access, logging, retention, destruction, disposal, incident management, and breach notification.

2.3.2. Each classification will have labeling requirements.

2.3.3. The Office of Information Security is responsible for the development and implementation of labeling and handling standards.

2.3.4. All employees, contractors, and affiliates will be provided or have access to written documentation that clearly describes the labeling and handling standards.

2.3.5. All employees, contractors, and affiliates will be provided with a resource that questions can be directed to.

2.3.6. All employees, contractors, and affiliates will be provided with a resource that violations can be reported to.

2.4. Inventory of Information System Assets

2.4.1. All information system assets shall be identified and documented with their classification, owner, location, and other details according to standards published by the Office of Information Security.

2.4.2. Company assets must be accounted for at all times.

2.4.3. The Office of Information Security will maintain the inventory documentation.

2.4.4. Copies of all inventory documentation will be included in the Business Continuity Plan.

Supporting Resources and Source Material

- ISO 27002:2013 Section 8 Asset Management
- NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-88 Guidelines for Media Sanitization

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Section 3: Human Resources Security

Overview

Information security is primarily a people-driven process; it is imperative that the Information Security Program be faithfully supported by information owners, custodians, and users. Personnel-related security controls, education, and acknowledgement of responsibilities need to be embedded in each stage of the employee lifecycle: recruitment, onboarding, user provisioning, orientation, career development, and termination.

Goals and Objectives for Section 3: Human Resources Security

- Ensure that company and candidate resources are protected during the recruitment process.
- Set the parameters for workforce background checks.
- Require an enterprise-wide user provisioning process.
- Define electronic monitoring activities, privacy rights, and employee consent.
- Require confidentiality and acceptable use agreements as a condition of employment.
- Ensure that disciplinary action, up to and including termination, is applied consistently and fairly according to the standard and attendant policies, procedures, and guidelines.
- Ensure that all employees, contractors, interns, and designated third parties receive training appropriate to their position throughout their tenure.

Human Resources Security Policy Index

3.0 Human Resources Security Policy

3.1. Recruitment

3.1.1. Any information that is classified as “protected” or “confidential” must not be included in job postings or job descriptions.

3.1.2. Candidates will not be allowed access to any secure area unless authorized in writing by the information owner.

3.1.3. All non-public information submitted by candidates must be classified as “protected” and handled in accordance with company handling standards.

3.1.4. Under no circumstances will the company request that candidates provide a password to social media, blog, web, or personal email accounts.

3.1.5. The Office of Information Security and the Office of Human Resources will be jointly responsible for the implementation and enforcement of this policy.

3.2. Personnel Screening

3.2.1. As a condition of employment, all employees, temporaries, and contractors must agree to and are subject to background screening that includes identity verification, confirmation of educational and professional credentials, credit check, and state and federal criminal check.

3.2.2. Comprehensive background screening will be conducted pre-hire. Criminal check will be conducted annually thereafter.

3.2.3. Background screening will be conducted in accordance with local, state, and federal law and regulations.

3.2.4. If the person will have access to “protected” or highly “confidential” information, additional screening may be required at the discretion of the information owner. This includes new personnel as well as employees who might be moved into such a position.

3.2.5. Background screening will be conducted and/or managed by the Human Resources department.

3.2.6. If temporary or contractor staff is provided by an agency or third party, the contract must clearly specify the agency or third-party responsibility for conducting background checks in accordance with this policy. Results must be submitted to the Human Resources department for approval.

3.3. User Provisioning

3.3.1. There will be defined and documented user provisioning process for granting and revoking access to information resources that includes but is not limited to account creation, account management including assignment of access rights and permissions, periodic review of access rights and permissions, and account termination.

3.3.2. The Office of Human Resources and the Office of Information Security are jointly responsible for the User Provisioning process.

3.4. Electronic Monitoring

3.4.1. The company reserves the right to monitor electronic activity on company-owned information systems including but not limited to voice, email, text and messaging communications sent, received, or stored, computer and network activity, and Internet activity including sites visited and actions taken.

3.4.2. The policy must be included in the employee acceptable use agreement and employees must acknowledge the policy by signing the agreement.

3.4.3. Whenever technically feasible, login banners and warning messages will remind users of this policy.

3.4.4. The Office of Human Resources and the Office of Information Security are jointly responsible for developing and managing electronic monitoring and employee notification

3.5. Employee Termination

3.5.1. Upon the termination of the relationship between the company and any employee, all access to facilities and information resources shall cease.

3.5.2. In the case of unfriendly termination, all physical and technical access will be disabled pre-notification.

3.5.3. In the case of a friendly termination including retirement, the Office of Human Resources is responsible for determining the schedule for disabling access.

3.5.4. Termination procedures are to be included in the User Provisioning Process.

3.5.5. The Office of Human Resources and the Office of Information Security are jointly responsible for the User Provisioning process.

3.6. Employee Agreements

3.6.1. All employees must be provided with and sign a confidentiality agreement as a condition of employment and prior to being provided any company information classified as protected, confidential, or internal use.

3.6.2. All employees must be provided with and sign an acceptable use agreement as a condition of employment and prior to being granted access to any company information or systems.

3.6.3. The documents provided to the employee will clearly state the employee's responsibilities during both employment and post-employment.

3.6.4. The employee's legal rights and responsibilities will be included in the document.

3.6.5. Legal counsel is responsible for developing, maintaining, and updating the confidentiality agreement.

3.6.6. The Office of Information Security is responsible for developing, maintaining, and updating the acceptable use agreement.

3.6.7. The Office of Human Resources is responsible for distributing the agreement and managing the acknowledgment process.

3.7. Information Security Training

3.7.1. The Human Resources department is responsible for information security training during the employee orientation phase. The training must include compliance requirements, company policies, and handling standards.

3.7.2. Subsequent training will be conducted at the departmental level. Users will be trained on the use of departmental systems appropriate to their specific duties to ensure the CIA of information is safeguarded.

3.7.3. Annual information security training will be conducted by the Office of Information Security. All staff is required to participate and attendance will be documented. At a minimum, training will include the following topics: current information security-related threats and risks, security policy updates, and reporting of security incidents.

3.7.4. The company will support the ongoing education of information security personnel by funding attendance at conferences, tuition at local colleges and universities, subscriptions to professional journals, and membership in professional organizations.

Supporting Resources and Source Material

- ISO 27002:2013 Section 7 Human Resources Security Management
- NIST SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Section 4: Physical and Environmental Security

Overview

Physical and environmental security blends information security requirements and traditional security control with the objective of preventing, deterring, and detecting, unauthorized access, damage, and interference to business premises and equipment.

Goals and Objectives for Section 4: Physical and Environmental Security

- Ensuring that the physical security of facilities is driven by an assessment methodology consistently applied.
- Defining a multi-tier classification system for defining workplace security requirements.
- Ensuring physical access to secure areas are restricted to authorized personnel.
- Ensuring facilities and rooms housing sensitive equipment are protected from physical and environmental danger, including fire, water, smoke, and theft.
- Codifying the company's commitment to sustainable computing and the minimization of power consumption.
- Creating a consistent practice for media and devices disposal and destruction.
- Creating a consistent practice for securing removable devices and media.

Physical and Environmental Security Policy Index

4.0 Physical and Environmental Security Policy

4.1. Physical Security Perimeter

4.1.1. The company will establish physical security perimeters around business premises.

4.1.2. An annual risk assessment of all existing business premises and information processing facilities will be performed to determine the type and strength of the security perimeter that is appropriate and prudent.

4.1.3. A risk assessment must be conducted on all new sites under consideration prior to building plans being finalized.

4.1.4. The Office of Facilities Management in conjunction with the Office of Information Security will conduct the risk assessment.

4.1.5. Risk assessment results and recommendations are to be submitted to the COO.

4.1.6. The Office of Facilities Management is responsible for the implementation and maintenance of all physical security perimeter controls.

4.2. Physical Entry Controls

4.2.1. Access to all non-public company locations will be restricted to authorized persons only.

4.2.2. The Office of Human Resources is responsible for providing access credentials to employees and contractors.

4.2.3. The Office of Facilities Management is responsible for visitor identification, providing access credentials, and monitoring access. All visitor management activities will be documented.

4.2.4. Employees and contractors are required to visibly display identification in all company locations.

4.2.5. Visitors are required to display identification in all non-public company locations.

4.2.6. Visitors are to be escorted at all times.

4.2.7. All personnel must be trained to immediately report unescorted visitors.

4.3. Workspace Classification

4.3.1. The company will use a three-tiered workspace classification schema consisting of secure, restricted, and public.

4.3.2. The company will publish definitions for each classification.

4.3.3. The criteria for each level will be maintained by and available from the Office of Facilities Management.

4.3.4. All locations will be associated with one of the three data classifications.

4.3.5. Classification assignment is the joint responsibility of the Office of Facilities Management and the Office of Information Security.

4.3.6. Each classification must have documented security requirements.

4.3.7. The COO must authorize exceptions.

4.4. Working in Secure Areas

4.4.1. All access to areas classified as “secure” will be continually monitored.

4.4.2. All work in areas classified as “secure” will be recorded. The recordings will be maintained for a period of 36 months.

4.4.3. Mobile data storage devices are prohibited and may not be allowed in areas classified as “secure” without the authorization of the system owner or Information Security Officer.

4.4.4. Audio or video recording equipment is prohibited and may not be allowed in areas classified as “secure” without the authorization of the system owner or the Office of Information Security.

4.4.5. This policy is in addition to workspace classification security protocols.

4.5. Clear Desk and Clear Screen

4.5.1. When left unattended during business hours, desks shall be clear of all documents classified as “protected” or “confidential.”

4.5.2. During non-business hours, all documents classified as “protected” or “confidential” will be stored in a secure location.

4.5.3. While in use, device displays of any type must be situated to not allow unauthorized viewing.

4.5.4. When left unattended during business hours, device displays should be cleared and locked to prevent viewing.

4.5.5. “Protected” and “confidential” documents should only be printed to assigned printers. Print jobs should be retrieved immediately.

4.5.6. Scanners, copiers, and fax machines must be locked when not in use and require user codes to operate.

4.6. Power Consumption Policy

4.6.1. The company is committed to sustainable computing and the minimization of power consumption.

4.6.2. All computing devices purchased must be Energy Star® (or equivalent) certified.

4.6.3. All computing devices must be configured in power saver mode unless the setting degrades performance.

4.6.4. A bi-annual assessment must be conducted by the Office of Facilities Management to determine the best method(s) to provide clean, reliable Data Center power.

4.6.5. Data Center equipment must be protected by damage caused by power fluctuations or interruptions.

4.6.6. Data Center power protection devices must be tested on a scheduled basis for functionality and load capacity. A log must be kept of all service and routine maintenance.

4.6.7. Data Center generators must be tested regularly according to manufacturer's instructions. A log must be kept of all service and routine maintenance.

4.7. Data Center and Communications Facilities Environmental Safeguards

4.7.1. Smoking, eating, and drinking is not permitted in Data Center and Communications Facilities.

4.7.2. Servers and communications equipment must be located in areas free from physical danger.

4.7.3. Servers and communications must be protected by uninterruptable power supplies and backup power sources.

4.7.4. Appropriate fire detection, suppression, and fighting equipment must be installed and/or available in all Data Center and Communications Facilities.

4.7.5. Appropriate climate control systems must be installed in all Data Center and Communications Facilities.

4.7.6. Emergency lighting must engage automatically during power outages at all Data Center and Communications Facilities.

4.7.7. The Office of Facilities Management is responsible for assessing the Data Center and Communications Facilities environmental requirements and providing the recommendations to the COO.

4.7.8. The Office of Facilities Management is responsible for managing and maintaining the Data Center and Communications Facilities climate control, fire, and power systems.

4.8. Secure Disposal Policy

4.8.1. The Office of Facilities Management and the Office of Information Security are jointly responsible for determining the disposal standards for each classification of information.

4.8.2. Devices or media containing "protected" or "confidential" information must not be sent off-site for repair and/or maintenance.

4.8.3. The standards for the highest classification must be adhered to when the device or media contains multiple types of data.

4.8.4. A chain of custody must be maintained for the destruction of "protected" and "confidential" information.

4.8.5. A Certificate of Destruction is required for third-party destruction of devices or media that contains "protected" and "confidential" information.

4.8.6. Disposal of media and equipment shall be done in accordance with all applicable state and federal environmental disposal laws and regulations.

4.9. Mobile Device and Media Security

4.9.1. All company-owned and employee-owned mobile devices and media that store or have the potential to store information classified as "protected" or "confidential" must be encrypted.

4.9.2. Whenever feasible, an anti-theft technology solution must be deployed that enables remote locate, remote lock, and remote delete/wipe functionality.

4.9.3. Loss or theft of a mobile device or media must be reported immediately to the Office of Information Security.

Supporting Resources and Source Material

- ISO 27002:2013 Section 11 Physical and Environmental Security
- NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-88 Guidelines for Media Sanitization

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Section 5: Communications and Operations Security

Overview

Communications and Operations Security addresses information security in the context of internal and outsourced information technology operations including Data Center operations, vulnerability management, protection against data loss, evidence-based logging, and vendor management.

Goals and Objectives for Section 5: Communications and Operations Security

- Require documented standard operating procedures (SOPs).
- Minimize harm and maximize success associated with making changes to information systems or processes.
- Ensure that operating system and application code vulnerabilities are addressed through the timely deployment of security patches.
- Ensure a company-wide effort to prevent, detect, and contain malicious software.
- Minimize the risk of interrupted business operations.
- Ensure there is a process in place to periodically review system access in order to confirm that unauthorized access has been prevented effectively.
- Extend organizational requirements to service providers.

Communications and Operations Policy Index

5.0 Communications and Operations Policy

5.1. Standard Operating Procedures (SOPs)

5.1.1. The Office of Information Technology is responsible for the publication and distribution of information systems related SOPs.

5.1.1.1. Information system custodians are responsible for developing and testing the procedures.

5.1.1.2. Information system owners are responsible for authorization and ongoing review.

5.1.2. The Office of Information Security is responsible for the authorization, publication, distribution, and review of information security-related SOPs.

5.1.2.1. Information security custodians are responsible for developing and testing the procedures.

5.2. Operational Change Control

5.2.1. The Office of Information Technology is responsible for maintaining a documented change control process that provides an orderly method in which changes to the information systems and processes are requested and approved prior to their installation and/or implementation. Changes to information systems include but are not limited to:

5.2.1.1. Vendor-released operating system, software application and firmware patches, updates and upgrades.

5.2.1.2. Updates and changes to internally developed software applications.

5.2.1.3. Hardware component repair/replacement.

5.2.1.4. Implementations of security patches are exempt from this process as long as they follow the approved patch management process.

5.2.2. The change control process must take into consideration the criticality of the system and the risk associated with the change.

5.2.3. Changes to information systems and processes considered critical to the operation of the company must be subject to pre-production testing.

5.2.4. Changes to information systems and processes considered critical to the operation of the company must have an approved rollback and/or recovery plan.

5.2.5. Changes to information systems and processes considered critical to the operation of the company must be approved by the Change Management Committee. Other changes may be approved by the Director of Information Systems, Chief Technology Officer (CTO), or Chief Information Officer (CIO).

5.2.6. Changes must be communicated to all impacted stakeholders.

5.2.7. In an emergency scenario, changes may be made immediately (business system interruption, failed server, and so on) to the production environment. These changes shall be verbally approved by a Manager supervising the affected area at the time of the change.

5.2.7.1. After the changes are implemented, the change must be documented in writing and submitted to the CTO.

5.3. Security Patch Management

5.3.1. Implementations of security patches are exempt from the organizational change management process as long as they follow the approved patch management process.

5.3.2. The Office of Information Security is responsible for maintaining a documented patch management process.

5.3.3. The Office of Information Technology is responsible for the deployment of all operating system, application, and device security patches.

5.3.4. Security patches will be reviewed and deployed according to applicability of the security vulnerability and/or identified risk associated with the patch or hot-fix.

5.3.5. Security patches will be tested prior to deployment in the production environment.

5.3.5.1. The CIO and the CTO have authority to waive testing based on the severity and applicability of the identified vulnerability.

5.3.6. Vendors who maintain company systems are required to adhere to the company patch management process.

5.3.7. If a security patch cannot be successfully applied, the COO must be notified. Notification must detail the risk to the organization.

5.4. Malicious Software (Malware) Protection

5.4.1. The Office of Information Technology is responsible for recommending and implementing prevention, detection, and containment controls.

5.4.2. Anti-malware software must be installed on all computer workstations, mobile devices, and servers to prevent, detect, and contain malicious software.

5.4.3. Any system found to be out-of-date with vendor-supplied virus definition and/or detection engines must be documented and remediated immediately or disconnected from the network until it can be updated.

5.4.4. The Office of Human Resources is responsible for developing and implementing malware awareness and incident reporting training.

5.4.5. All malware-related incidents must be reported to the Office of Information Security.

5.4.6. The Office of Information Security is responsible for incident management.

5.5. Data Replication

5.5.1. The Office of Information Security is responsible for design and oversight of the enterprise replication and backup strategy. Factors to be considered include but are not limited to impact, cost, and regulatory requirements.

5.5.2. Data contained on replicated or backup media will be protected at the same level of access control as the data on the originating system.

5.5.3. The Office of Information Technology is responsible for the implementation, maintenance, and ongoing monitoring of the replication and backup/restoration strategy.

5.5.4. The process must be documented.

5.5.5. The procedures must be tested on a scheduled basis.

5.5.6. Backup media no longer in rotation for any reason will be physically destroyed so that the data is unreadable by any means.

5.6. Email and Email Systems Security

5.6.1. The Office of Information Security is responsible for assessing the risk associated with email and email systems. Risk assessments must be performed at a minimum bi-annually or whenever there is a change trigger.

5.6.2. The Office of Information Security is responsible for creating email security standards including but not limited to attachment and content filtering, encryption, malware inspection, and distributed denial of service (DDoS) mitigation.

5.6.3. External transmission of data classified as "protected" or "confidential" must be encrypted.

5.6.4. Remote access to company email must conform to the corporate remote access standards.

5.6.5. Access to personal web-based email from the corporate network is not allowed.

5.6.6. The Office of Information Technology is responsible for implementing, maintaining, and monitoring appropriate controls.

5.6.7. The Office of Human Resources is responsible for providing email security user training.

5.7. Security Log Management

5.7.1. Devices, systems, and applications implemented by the company must support the ability to log activities including data access and configuration modifications.

5.7.1.1. Exceptions must be approved by the COO.

5.7.2. Access to logs must be restricted to individuals with a need-to-know.

5.7.3. Logs must be retained for a period of 12 months.

5.7.4. Log analysis reports must be retained for 36 months.

5.7.5. The Office of Information Security is responsible for:

5.7.5.1. Developing log management standards, procedures, and guidelines.

5.7.5.2. Prioritizing log management appropriately throughout the organization.

5.7.5.3. Creating and maintain a secure log management infrastructure.

5.7.5.4. Establishing log analysis incident response procedures.

5.7.5.5. Providing proper training for all staff with log management responsibilities.

5.7.6. The Office of Information Technology is responsible for:

5.7.6.1. Managing and monitoring the log management infrastructure.

5.7.6.2. Proactively analyzing log data to identify ongoing activity and signs of impending problems.

5.7.6.3. Providing reports to the Office of Information Security.

5.8. Service Provider Management

5.8.1. A service provider is defined as a vendor, contractor, business partner, or affiliate, who stores, processes, transmits, or accesses company information or company information systems.

5.8.2. The Office of Risk Management is responsible for overseeing the selection, contract negotiations, and management of service providers.

5.8.3. The Office of Risk Management will be responsible for conducting applicable service provider risk assessments.

5.8.4. Due diligence research must be conducted on all service providers. Depending upon risk assessment results, due diligence research may include but is not limited to financial soundness review, internal Information Security Policy and control environment review, and review of any industry standard audit and/or testing of information security-related controls.

5.8.5. Service provider systems are required to meet or exceed internal security requirements. Safeguards must be commensurate with the classification of data and the level of inherent risk.

5.8.6. Contracts and/or agreements with service providers must specifically require them to protect the CIA of all company, customer, and proprietary information that is under their control.

5.8.7. Contracts and/or agreements must include the following:

5.8.7.1. Notification requirements for suspected or actual compromise or system breach.

5.8.7.2. A statement that acknowledges the service provider's obligation to comply with all applicable state and federal regulations.

5.8.7.3. Provision for periodic security reviews/audits of the service provider environment.

5.8.7.4. Provision requiring service providers to disclose the use of contractors.

5.8.7.5. As applicable, a clause related to the proper destruction of records containing customer or proprietary information when no longer in use or if the relationship is terminated.

5.8.8. To the extent possible and practical, contractual performance will be monitored and/or verified.

5.8.8.1. Oversight is the responsibility of the business process owner.

Supporting Resources and Source Material

- ISO 27002:2013 Section 12 Operations Security
- ISO 27002:2013 Section 13 Communications Security
- ISO 27002:2013 Section 15 Supplier Relationships
- NIST SP 800-40 Creating a Patch and Vulnerability Management Program
- NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-45 Guidelines on Electronic Mail Security
- NIST SP 800-92 Guide to Computer Security Log Management
- NIST SP 800-42 Guideline on Network Security Testing

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Section 6: Access Control Management

Overview

Access controls are security features that govern how users and processes communicate and interact with systems and resources. The objective of implementing access controls is to ensure that authorized users and processes are able to access information and resources while unauthorized users and processes are prevented from access to the same.

Goals and Objectives for Section 6: Access Control Management

- To require the positive identification of the person or system seeking access to secured information, information systems, or devices.
- To state the access control authorization principles of the organization.
- To ensure that access is granted only to authorized users and processes, and where appropriate, to provide users the minimum access required to perform a given role effectively.
- To logically group network assets, resources, and applications for the purpose of applying security controls.
- To define the requirements for the secure design, configuration, management, administration, and oversight of border devices.
- To assign responsibility and set the requirements for remote access connections to the internal network.
- To assign responsibility and set the requirements for teleworking.
- To ensure that there is a means to prevent and/or detect attempts to gain access to information resources by unauthorized entities.

Infrastructure Access Control Policy Index

6.0 Access Control Policy

6.1. Authentication Policy

6.1.1. Access to and use of information technology systems must require an individual to uniquely identify and authenticate him/herself to the resource.

6.1.2. Multi-user or shared accounts are allowed only when there is a documented and justified reason that has been approved by the Office of Information Security.

6.1.3. The Office of Information Security is responsible for managing an annual user account audit of network accounts, local application accounts, and web application accounts.

6.1.4. Data classification, regulatory requirements, the impact of unauthorized access, and the likelihood of a threat being exercised must all be considered when deciding upon the level of authentication required. The Office of Information Security will make this determination in conjunction with the information system owner.

6.1.5. Operating systems and applications will at a minimum be configured to require single-factor complex password authentication.

6.1.5.1. Password complexity will be defined in the company password standard.

6.1.5.2. The password standard will be published, distributed, and included in the acceptable use agreement.

6.1.5.3. The inability to technically enforce this standard does not negate the requirement.

6.1.6. Web applications that transmit, store, or process "protected" or "confidential", information must at a minimum be configured to require single-factor complex password authentication.

6.1.6.1. Passwords and PINs must be unique to the application.

6.1.6.2. Whenever feasible, multi-factor authentication must be implemented.

6.1.6.3. The inability to technically enforce this standard does not negate the requirement.

6.1.7. Exceptions to this policy must be approved by the Office of Information Security

6.1.8. All passwords must be encrypted during transmission and storage. Applications that do not conform to this requirement may not be used.

6.1.9. Any mechanism used for storing passwords must be approved by the Office of Information Security.

6.1.10. If any authentication mechanism has been compromised or is suspected of being compromised, users must immediately contact the Office of Information Security and follow the instructions given.

6.2. Access Control Authorization

6.2.1. Default access privileges will be set to "deny all."

6.2.2. Access to information and information systems must be limited to personnel and processes with a need-to-know to effectively fulfill their duties.

6.2.3. Access permissions must be based on the minimum required to perform job or program function.

6.2.4. Information and information system owners are responsible for determining access rights and permissions.

6.2.5. The Office of Information Security is responsible for enforcing an authorization process.

6.2.6. Permissions must not be granted until the authorization process is complete.

6.3. Network Segmentation

6.3.1. The network infrastructure shall be segregated into distinct segments according to security requirements and service function.

6.3.2. The Office of Information Security and the Office of Information Technology are jointly responsible for conducting annual Network Segment Risk Assessments. The results of the assessment will be provided to the COO.

6.3.3. Complete documentation of the network topology and architecture will be maintained by the Office of Information Technology including an up-to-date network diagram showing all internal (wired and wireless) connections, external connections, and endpoints, including the Internet.

6.4. Border Device Security

6.4.1. Border security access control devices shall be implemented and securely maintained to restrict access between networks that are trusted to varying degrees.

6.4.2. If any situation renders the Internet-facing border security devices inoperable, Internet service must be disabled.

6.4.3. The Office of Information Technology is responsible for designing, maintaining, and managing border security access control devices.

6.4.3.1. At the discretion of the COO, this function or part of may be outsourced to a Managed Security Service Provider (MSSP).

6.4.3.2. Oversight of internal or MSSP border security device administrators is assigned to the Office of Information Security.

6.4.4. The Office of Information Security is responsible for approving border security access control architecture, configuration, and rule-sets.

6.4.5. The default policy for handling inbound and outbound traffic should be to deny all.

6.4.5.1. The types of network traffic that must always be denied without exception will be documented in the border device security standards.

6.4.5.2. Rule-sets must be as specific and simple as possible. Rule-set documentation will include the business justification for allowed traffic.

6.4.5.3. All configuration and rule-set changes are subject to the organizational change management process.

6.4.5.4. All rule-set modifications must be approved by the Office of Information Security.

6.4.6. All border security access control devices must be physically located in a controlled environment, with access limited to authorized personnel.

6.4.7. To support recovery after failure or natural disaster, the border security device configuration, policy, and rules must be backed up or replicated on a scheduled basis as well as before and after every configuration change.

6.4.8. Border devices must be configured to log successful and failed activity as well as configuration changes.

6.4.8.1. Border device logs must be reviewed daily by the Office of Information Technology or MSSP and an activity report submitted to the Office of Information Security.

6.4.9. Configuration and rule-set reviews must be conducted annually.

6.4.9.1. The review is to be conducted by an external independent entity.

6.4.9.2. Selection of the vendor is the responsibility of the Audit Committee.

6.4.9.3. Testing results are to be submitted to the COO.

6.4.10. External penetration testing must at a minimum be performed semi-annually.

6.4.10.1. The testing is to be conducted by an external independent entity.

6.4.10.2. Selection of the vendor is the responsibility of the Audit Committee.

6.4.10.3. Testing results are to be submitted to the COO.

6.5. Remote Access

6.5.1. The Office of Information Security is responsible for approving remote access connections and security controls.

6.5.2. The Office of Information Technology is responsible for managing and monitoring remote access connection.

6.5.3. Remote access connections must use 128-bit or greater encryption to protect data in transit (that is, VPN, SSL, SSH).

6.5.4. Multifactor authentication must be used for remote access.

6.5.4.1. Whenever technically feasible, one factor shall be "out-of-band."

6.5.5. Remote equipment must be company-owned and configured in accordance with company workstation security standards.

6.5.6. Business partners and vendors wishing to obtain approval for remote access to computing resources must have access approved by the COO. Their company sponsor is required to provide a valid business reason for the remote access to be authorized.

6.5.7. Employees, business partners, and vendors approved for remote access must be presented with and sign a Remote Access Agreement that acknowledges their responsibilities prior to being granted access.

6.5.8. Remote access devices must be configured to log successful and failed activity as well as configuration changes.

6.5.8.1. Remote access logs must be reviewed daily by the Office of Information Technology or designee and an activity report submitted to the Office of Information Security.

6.5.9. Remote access user lists must be reviewed quarterly by the Office of Human Resources.

6.5.9.1. The result of the review must be reported to both the Office of Information Security and Office of Information Technology.

6.5.10. External penetration testing must at a minimum be performed semi-annually.

6.5.10.1. The testing is to be conducted by an external independent entity.

6.5.10.2. Selection of the vendor is the responsibility of the Audit Committee.

6.5.10.3. Testing results are to be submitted to the COO.

6.6. Teleworking Policy

6.6.1. Teleworking schedule must be requested in writing by management to and authorized by the Office of Human Resources.

6.6.2. The Office of Human Resources is responsible for notifying the Office of Information Security and Office of Information Technology when a user is granted or denied teleworking privileges.

6.6.3. Teleworking equipment including connectivity devices must be company-owned and configured in accordance with company security standards.

6.6.4. The Office of Information Technology is responsible for managing, maintaining, and monitoring the configuration of and the connection to the teleworking location.

6.6.5. Remote access will be granted in accordance with the Remote Access policy and standards.

6.6.6. The teleworker is responsible for the physical security of the telecommuting location.

6.6.7. Local storage of information classified as “protected” or “confidential” must be authorized by the Office of Information Security.

6.6.8. Monitoring the teleworker is the responsibility of their immediate supervisor.

6.7. User Access Control and Authorization

6.7.1. Default user access permissions will be set to “deny all” prior to the appropriation of specific permissions based on role and/or job function.

6.7.2. Access to company information and systems shall only be authorized for workforce personnel with a need-to-know to perform their job function(s).

6.7.3. Access shall be restricted to the minimal amount required to carry out the business requirement of the access.

6.7.4. An authorization process must be maintained. Permissions must not be granted until the authorization process is complete.

6.7.5. Information owners are responsible for annually reviewing and reauthorizing user access permissions to data classified as “protected” or “confidential.”

6.7.6. The Office of Information Security is responsible for managing the review and reauthorization process.

6.7.7. Annual report of completion will be provided to the Audit Committee.

6.8. Administrative and Privileged Accounts

6.8.1. Request for assignment of administrator-level accounts or changes to privileged group membership must be submitted to the Office of Information Security and approved by the COO.

6.8.2. The Office of Information Security is responsible for determining the appropriate use of administrator segregation of duties and dual controls.

6.8.3. Administrative and privileged user accounts will only be used when performing duties requiring administrative or privileged access.

6.8.4. All administrative and privileged account holders will have a second user account for performing any function where administrative or privileged access is not required.

6.8.5. User accounts assigned to contractors, consultants, or service providers who require administrative or privileged access will be enabled according to documented schedule and/or formal request, and disabled at all other times.

6.8.6. Administrative and privileged account activity will be logged daily and reviewed by the Office of Information Security.

6.8.7. Administrative and privileged account assignments will be reviewed quarterly by the Office of Information Security.

6.9. Monitoring System Access and Use

6.9.1. The Office of Information Technology, the Office of Information Security, and the Office of Human Resources are jointly responsible for determining the extent of logging and analysis required for information systems storing, processing, transmitting, or providing access to information classified as “confidential” or “protected.” However, at a minimum, the following must be logged:

6.9.1.1. Successful and failed network authentication.

6.9.1.2. Successful and failed authentication to any application that stores or processes information classified as “protected.”

6.9.1.3. Network and application administrative or privileged account activity.

6.9.2. Exceptions to the above list must be authorized by the COO.

6.9.3. Access logs must be reviewed daily by the Office of Information Technology or designee and an activity report submitted to the Office of Information Security.

Supporting Resources and Source Material

- ISO 27002:2013 Section 9 Access Control
- NIST SP 800-40 Creating a Patch and Vulnerability Management Program
- NIST SP 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems
- NIST SP 800-41 R1 Guidelines on Firewalls and Firewall Policy
- NIST SP 800-46 R1 Guide to Enterprise Telework and Remote Access Security
- NIST SP 800-77 Guide to IPsec VPNs
- NIST SP 800-114 User’s Guide to Securing External Devices for Telework and Remote Access
- NIST SP 800-113 Guide to SSL VPNs

- NIST SP 880-114 User's Guide to Securing External Devices for Telework and Remote Access
- NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks (WLANs)

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Section 7: Information Systems Acquisition, Development, and Maintenance

Overview

Information Systems Acquisition, Development, and Maintenance focuses on (1) the lifecycle of information systems and components and (2) internal software development. The purpose of this section is to require secure practices from initiation through destruction.

Goals and Objectives for Section 7: Information Systems Acquisition, Development, and Maintenance

- Ensure a structured and standardized process for all phases of system development/acquisition efforts that includes security considerations, requirements, and testing.
- Define the requirements for the implementation and maintenance of commercial and open source software.
- Define code and application development security requirements.
- Assign responsibility for key management and cryptographic standards.

Information Systems Acquisition, Development, and Maintenance Policy Index

7.1. System Development Lifecycle (SDLC)

7.2. System Implementation and Maintenance

7.3. Application Development

7.4. Key Management

7.0 Information Systems Acquisition, Development, and Maintenance Policy

7.1. System Development Lifecycle (SDLC)

7.1.1. The Office of Information Technology is responsible for adopting, implementing, and requiring compliance with an SDLC process and workflow. The SDLC must define initiation, development/acquisition, implementation, operations, and disposal requirements.

7.1.2. At each phase, security requirements must be evaluated and, as appropriate, security controls tested.

7.1.3. The system owner in conjunction with the Office of Information Security is responsible for defining system security requirements.

7.1.4. The system owner in conjunction with the Office of Information Security is responsible for authorizing production systems prior to implementation.

7.1.5. If necessary, independent experts may be brought in to evaluate the project or any component thereof.

7.2. System Implementation and Maintenance

7.2.1. Operating systems and applications (collectively referred to as "system") implementation and updates must follow the company change management process.

7.2.2. Without exception, alpha, beta, or prerelease applications must not be deployed on production systems.

7.2.3. It is the joint responsibility of the Office of Information Security and the Office of Information Technology to test system implementation and updates prior to deployment in the production environment.

7.2.4. The Office of Information Technology is responsible for budgeting for and maintaining a test environment that is representative of the production environment.

7.2.5. Without exception, data classified as "protected" must not be used in a test environment unless it has been de-identified.

7.2.5.1. It is the responsibility of the Office of Information Security to approve the de-identification schema.

7.3. Application Development

7.3.1. System owners are responsible for oversight of secure code development.

7.3.2. Security requirements must be defined and documented during the application development initiation phase.

7.3.3. Code development will be done in accordance with industry best practices.

7.3.4. Developers will be provided with adequate training, resources, and time.

7.3.5. At the discretion of the system owner and with the approval of the Office of Information Security, third parties may be engaged to design, develop, and test internal applications.

7.3.6. All code developed or customized must be tested and validated during development, prior to release, and whenever a change is implemented.

7.3.7. The Office of Information Security is responsible for certifying the results of testing and accreditation to move to the next phase.

7.4. Key Management

7.4.1. The Office of Information Security is responsible for key management including but not limited to algorithm decisions, key length, key security and resiliency, requesting and maintaining digital certificates, as well as user education.

7.4.2. The Office of Information Security will publish cryptographic standards.

7.4.3. The Office of Information Technology is responsible for implementation and operational management of cryptographic technologies.

7.4.4. Without exception, encryption is required whenever "protected" or "confidential" information is transmitted externally. This includes email and files transfer. The encryption mechanism must be NIST approved.

7.4.5. Without exception, all portable media that stores or has the potential to store "protected" or "confidential" information must be encrypted. The encryption mechanism must be NIST approved.

7.4.6. Data at rest must be encrypted regardless of media when required by state and/or federal regulation or contractual agreement.

7.4.7. At all times, passwords and PINs must be stored and transmitted as cipher text.

Supporting Resources and Source Material

- ISO 27002:2013 Section 10 Cryptography
- ISO 27002:2013 Section 10 Information Systems Acquisition, Development, and Maintenance
- NIST SP 880-57 Recommendations for Key Management
- NIST SP 800-64 Security Considerations in the System Development Lifecycle
- NIST SP 800-111 Guide to Storage Encryption Technologies for End Users

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Section 8: Incident Management

Overview

It is critical that as an organization we have the capability to respond quickly, minimize harm, comply with breach-related state laws and federal regulations, and maintain their composure in the face of an information security-related incident. The purpose of this section is to define incident management requirements.

Goals and Objectives for Section 8: Incident Management

- Define organizational criteria pertaining to an information security incident.
- Classify incidents by severity and assigned response and notification requirements.
- Ensure that information security incidents are responded to, managed, and reported in a consistent and effective manner.
- Vest authority in those charged with responding to and/or managing an information security incident.
- Ensure that evidence is handled in accordance with legal requirements.
- Ensure compliance with all applicable laws, regulations, and contractual obligations, timely communications with customers, and internal support for the process.

Incident Management Policy Index

8.0 Incident Management Policy

8.1. Incident Definition

8.1.1. An information security incident is an event that has the potential to adversely impact the company, our clients, our business partners, and/or the public-at-large.

8.1.2. An information security incident is defined as one or more of the following:

8.1.2.1. Actual or suspected unauthorized access to, compromise of, acquisition of, or modification of protected client or employee data including but not limited to: personal identification numbers, such as social security numbers (SSNs), passport numbers, driver's license numbers, financial account or credit card information, including account numbers, card numbers, expiration dates, cardholder name, service codes, or healthcare/medical information.

8.1.2.2. Actual or suspected event that has the capacity to disrupt the availability of services provided to our clients.

8.1.2.3. Actual or suspected unauthorized access to, compromise of, acquisition of, or modification of company intellectual property.

8.1.2.4. Actual or suspected event that has the capacity to disrupt the company's ability to provide internal computing and network services.

8.1.2.5. Actual or suspected event that is in violation of legal or statutory requirements.

8.1.2.6. Actual or suspected event not defined above that warrants incident classification as determined by management.

8.1.3. All employees, contractors, consultants, vendors, and business partners are required to report known or suspected information security incidents.

8.1.4. This policy applies equally to internal and third-party incidents.

8.2. Information Security Incident Classification

8.2.1. Incidents are to be classified by severity relative to the impact it has on an organization. If there is ever a question as to which level is appropriate, the company must err on the side of caution and assign the higher severity level.

8.2.2. Level 1 incidents are defined as those that could cause significant harm to the business, customers, or the public and/or are in violation of corporate law, regulation, or contractual obligation.

8.2.2.1. Level 1 incidents must be responded to immediately upon report.

8.2.2.2. The CEO, the COO, legal counsel, and CISO must be informed of Level 1 incidents.

8.2.3. Level 2 incidents are defined as compromise of or unauthorized access to non-critical systems or information; detection of precursor to a focused attack; believed threat of an imminent attack, or any act that is a potential violation of law, regulation, or contractual obligation.

8.2.3.1. Level 2 incidents must be responded to within 4 hours.

8.2.3.2. The COO, legal counsel and the CISO must be informed of Level 2 incidents.

8.2.4. Level 3 incidents are defined as situations that can be contained and resolved by the information system custodian, data/process owner, or human resources personnel. There is no evidence or suspicion of harm to customer or proprietary information, processes, or services.

8.2.4.1. Level 3 incidents must be responded to within 24 business hours.

8.2.4.2. The Information Security Officer must be informed of Level 3 incidents.

8.3. Information Security Incident Response Program

8.3.1. An Incident Response Plan (IRP) shall be maintained to ensure that information security incidents are responded to, managed, and reported in a consistent and effective manner.

8.3.2. The Office of Information Security is responsible for the establishment and maintenance of an IRP.

8.3.3. The IRP will at a minimum include instructions, procedures, and guidance related to preparation, detection and investigation, initial response, containment, eradication and recovery, notification, closure and post-incident activity, and documentation and evidence handling.

8.3.4. In accordance with the Information Security Incident Personnel Policy, the IRP will further define personnel roles and responsibilities including but not limited to Incident Response Coordinators, Designated Incident Handlers, and Incident Response Team members.

8.3.5. All employees, contractors, consultants, and vendors will receive incident response training appropriate to their role.

8.3.6. The IRP must be annually authorized by the Board of Directors.

8.4. Incident Response Authority

8.4.1. The CISO has the authority to appoint Incident Response Coordinators, Designated Incident Handlers, and Incident Response Team members.

8.4.2. All responders must receive training commensurate with their role and responsibilities.

8.4.3. All responders must participate in recurring drills and exercises.

8.4.4. During a security incident, as well as during drills and exercises, incident management and incident response-related duties supersede normal duties.

8.4.5. The COO and/or legal counsel has the authority to notify law enforcement or regulatory officials.

8.4.6. The COO, Board of Directors, and/or legal counsel have the authority to engage outside personnel including but not limited to forensic investigators, experts in related fields such as security, technology, and compliance, and specialized legal counsel.

8.5. Evidence Handling and Usage

8.5.1. All evidence, logs, and data associated with the incident must be handled as follows:

8.5.1.1. All evidence, logs, and data associated with the incident must be labeled.

8.5.1.2. All evidence, logs, and data associated with the incident should be placed in tamper-resistant containers, grouped together, and put in a limited access location.

8.5.1.3. All evidence handling must be recorded on a Chain of Custody.

8.5.2. Unless otherwise instructed by legal counsel or law enforcement officials, all internal digital evidence should be handled in accordance with the procedures described in the United States Department of Justice, National Institute of Justice, April 2008, "Electronic Crime Scene Investigation: A Guide for First Responders, 2nd edition." If not possible, deviations must be noted.

8.5.3. Unless otherwise instructed by legal counsel or law enforcement officials, subsequent internal forensic investigation and analysis should follow United States Department of Justice, National Institute of Justice, April 2004, "Forensic Examination of Digital Evidence; Guide for Law Enforcement" guidelines. If not possible, deviations must be noted.

8.5.4. Executive Management and the Designated Incident Handler have the authority to engage outside expertise for forensic evidence handling investigation and analysis.

8.5.5. Exceptions to this policy can only be authorized by legal counsel.

8.6. Data Breach Reporting and Notification

8.6.1. It is the intent of the company to comply with all information security breach-related laws, regulations, and contractual obligations.

8.6.2. Executive Management has the authority to engage outside expertise for legal counsel, crisis management, public relations, and communications.

8.6.3. Affected customer and business partners will be notified as quickly as possible of a suspected or known compromise of personal information. The company will provide regular updates as more information becomes known.

8.6.4. Based upon applicable laws, legal counsel in collaboration with the CEO will make the determination regarding the scope and content of customer notification.

8.6.5. Legal counsel and the marketing/PR department will collaborate on all internal and external notifications and communications. All publications must be authorized by Executive Management.

8.6.6. Customer service must staff appropriately to meet the anticipated demand for additional information.

8.6.7. The COO is the official spokesperson for the organization. In his/her absence, legal counsel will function as the official spokesperson.

Supporting Resources and Source Material

- ISO 27002:2013 Section 16 Information Security Incident Management
- NIST SP 880-61 Computer Security Incident Handling Guide
- NIST SP 800-66 Guide to Integrating Forensic Techniques into Incident Response

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Section 9: Business Continuity

Overview

The objective of the Business Continuity Management is to ensure the continued operation and secure provision of essential services during a disruption of normal operating conditions. The purpose of this section is to define business continuity preparedness, response, and recovery capabilities.

Goals and Objectives for Section 9: Business Continuity

- Demonstrate the organization's commitment to emergency preparedness and business continuity.
- Require and assign responsibility for an annual business impact assessment (BIA).
- Require the organization to have a Business Continuity Plan.
- Assign business continuity management responsibilities.
- Ensure that the organization is prepared to respond to an emergency situation.
- Ensure that the organization can continue to provide essential services during the recovery period.
- Ensure that the organization can recover infrastructure, systems, and facilities damaged during a disaster.
- Codify testing and maintenance requirements and responsibility.

Business Continuity Policy Index

9.0 Business Continuity Policy

9.1. Emergency Preparedness

9.1.1. An emergency preparedness and business continuity strategy that ensures the safety of employees and customers, enables the company to perform essential functions absent normal operating conditions, protects organizational assets, and meets regulatory requirements is an organizational priority.

9.1.2. The company will designate necessary resources to develop and maintain emergency preparedness and Business Continuity Plans and procedures.

9.2. Business Impact Assessment (BIA)

9.2.1. The COO is responsible for scheduling an enterprise-wide annual BIA. System owner participation is required.

9.2.2. The BIA will identify *essential* services and processes. Essential is defined as meeting one or more of the following criteria:

9.2.2.1. Required by law, regulation, or contractual obligation.

9.2.2.2. Disruption would be a threat to public safety.

9.2.2.3. Disruption would impact the health and well-being of employees.

9.2.2.4. Disruption would result in irreparable harm to customers or business partners.

9.2.2.5. Disruption would result in significant or unrecoverable financial loss.

9.2.3. For each essential service and/or process, the maximum tolerable downtime (MTD) will be documented. The MTD is the total length of time an essential function or process can be unavailable without causing significant harm to the business.

9.2.4. For each essential service and/or process, supporting infrastructure, devices/information systems and dependencies will be identified.

9.2.5. Recovery time objectives (RTOs) and recovery point objectives (RPOs) for supporting infrastructure and devices/information systems will be documented.

9.2.6. Current capability and capability delta will be identified. Deviations that put the organization at risk must be reported to the Board of Directors.

9.2.7. The COO, the CIO, and the Business Continuity Team are jointly responsible for aligning the BIA outcome with the Business Continuity Plan.

9.3. Business Continuity Plan

9.3.1. The company's business continuity strategy will be documented in a Business Continuity Plan. The plan shall include plans, procedures, and ancillary documentation related to emergency preparedness, disaster preparation, response, contingency operations, recovery, resumption, training, testing, and plan maintenance.

9.4. Business Continuity Management

9.4.1. The Board of Directors is responsible for authorizing the Business Continuity Plan. Reference to the Business Continuity Plan is inclusive of plans, procedures, and ancillary documentation related to disaster preparation, response, contingency operations, recovery, resumption, training, testing, and plan maintenance.

9.4.1.1. The Board must be appraised on a timely basis of any material changes to the business continuity strategy.

9.4.2. The COO or designee is responsible for the development, maintenance, and management of the business continuity strategy and plan.

9.4.3. The Chief Financial Officer will include business continuity expenses in the annual operating budget.

9.4.4. The Office of Information Technology is responsible for designing and supporting resilient systems and for the recovery of information and information systems in a disaster situation.

9.4.5. Senior managers are responsible for defining the operational needs of their departments and for creating and maintaining functional departmental contingency procedures.

9.4.6. The COO will appoint the Business Continuity Team chairperson. The chairperson will appoint members of the Business Continuity Team. The team must include representatives of key functional areas including but not limited to operations, communications, finance, information technology, information security, physical security, and facilities management. Team members are responsible for designating a backup to serve in their absence.

9.4.7. Business Continuity Team responsibilities include active participation in business continuity preparation, response, recovery, and resumption activities. At its discretion, the Business Continuity Team may create sub-teams and assign responsibilities.

9.4.8. The CEO has the authority to declare an emergency, activate the plan, and contact/assemble the Business Continuity Team.

9.4.8.1. In her/his absence, the COO has the authority to declare an emergency, activate the plan, and contact/assemble the Business Continuity Team.

9.4.8.2. In her/his absence, the Chief Financial Officer has the authority to declare an emergency, activate the plan, and contact/assemble the Business Continuity Team.

9.4.8.3. If none of the above listed are available, the Business Continuity Team chair in consultation with the Chairman of the Board of Directors has the authority to declare an emergency, activate the plan, and contact/assemble the Business Continuity Team.

9.4.9. The Business Continuity Team will be the authoritative body during emergency response and recovery periods. Officers and employees will continue to conduct the affairs of the company under the guidance of the team leadership, except in matters, which by statute require specific approval of the Board of Directors, or to conform to any governmental directives.

9.5. Emergency Response Plan

9.5.1. The COO is responsible for developing and maintaining the Emergency Response Plan. The Emergency Response Plan is a component of the enterprise Business Continuity Plan.

9.5.2. The objective of the Emergency Response Plan is to protect the health and safety of employees, customers, first responders, and the public at large, minimizing damage to property and the environment and set in motion response, contingency, and recovery operations.

9.5.3. The Emergency Response Plan must at a minimum address organizational alerts and notification, disaster declaration, internal and external communication channels, command and control centers, relocation options, and decision making authority.

9.5.4. Ancillary to the Response Plan are the Occupant Emergency Plan (OEP) and Crisis Communication Plan (CCP). Both plans may be utilized in conjunction with and/or referenced by the Response Plan.

9.5.5. The Office of Human Resources is responsible for maintaining the OEP.

9.5.6. The Office of Communications and Marketing is responsible for maintaining a CCP.

9.5.7. Personnel responsible for response operations must receive appropriate training.

9.5.8. Response plans and procedures must be audited in accordance with the schedule set forth by the Business Continuity Team.

9.5.9. Response procedures must be tested in accordance with the schedule set forth by the Business Continuity Team.

9.6. Operational Contingency Plan

9.6.1. Business process owners are responsible for developing and maintaining Operational Contingency Plans. Operational Contingency Plans are a component of the enterprise Business Continuity Plan.

9.6.2. The Operational Contingency Plans must include strategies and procedures for providing essential services as determined by the BIA during the recovery operations.

9.6.3. The amount of procedural detail required should be enough that competent personnel familiar with the service or process could perform the alternate operation.

9.6.4. External system dependencies and relevant contractual agreements must be reflected in the contingency plan.

9.6.5. Personnel responsible for contingency operations must receive appropriate training.

9.6.6. Contingency plans and procedures must be audited in accordance with the schedule set forth by the Business Continuity Team.

9.6.7. Contingency procedures must be tested in accordance with the schedule set forth by the Business Continuity Team.

9.7. Disaster Recovery Plan

9.7.1. The Office of Information Technology and the Office of Facilities Management are responsible for their respective Disaster Recovery Plans. Disaster Recovery Plans are a component of the enterprise Business Continuity Plan.

9.7.2. The Disaster Recovery Plan must include recovery strategies and procedures for systems and facilities as determined by the BIA.

9.7.3. Modifications to the recovery plan must be approved by the COO.

9.7.4. The amount of procedural detail required should be enough that competent personnel familiar with the environment could perform the recovery operation.

9.7.5. External system dependencies and relevant contractual agreements must be reflected in the recovery plan.

9.7.6. Personnel responsible for recovery operations must receive appropriate training.

9.7.7. Recovery plans and procedures must be audited in accordance with the schedule set forth by the Business Continuity Team.

9.7.8. Recovery procedures must be tested in accordance with the schedule set forth by the Business Continuity Team.

9.8. Continuity Testing and Maintenance

9.8.1. Reference to the Business Continuity Plan is inclusive of plans, procedures, and ancillary documentation related to disaster preparation, response, contingency operations, recovery, resumption, training, testing, and plan maintenance.

9.8.2. The COO or designee is responsible for maintenance of the Business Continuity Plan.

9.8.3. The COO or designee will conduct an annual review of the Business Continuity Plan.

9.8.4. The Business Continuity Team is responsible for publishing an annual testing schedule and managing the test plan.

9.8.4.1. The COO will report the results to the Board of Directors.

9.8.5. Internal audit is tasked with managing and selecting an independent firm to conduct an annual audit of the Business Continuity Plan.

9.8.5.1. The independent audit firm will report the results to the Board of Directors or designated committee.

Supporting Resources and Source Material

- ISO 27002:2013 Section 14 Business Continuity Management
- NIST SP 880-34 Contingency Planning Guide for Information Technology Systems
- NIST SP 800-84 Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities

Lead Author

Name: <insert name>

Contact Information: <insert contact information>

Appendix C

Information Systems Acceptable Use Agreement and Policy

Information Systems Acceptable Use Agreement

Effective security is a civic responsibility and a team effort involving the participation and support of every information systems user and affiliate who deals with information and/or information systems. It is the responsibility of every information systems user and affiliate to know, understand, and adhere to our Information Systems Acceptable Use Policy and to conduct their activities accordingly.

Distribution

All information systems users shall receive a copy of the Information Systems Acceptable Use Policy during orientation and thereafter on an annual basis. Users must acknowledge their acceptance by signing an Information Systems Acceptable Use Agreement within a time period to be specified by management. Any user who does not sign the acceptable use statement will have all access to information systems removed and may have their employment terminated.

Information Systems Acceptable Use Agreement

I certify that I have read and fully understand the Information Systems Acceptable Use Policy. I understand and acknowledge my obligations and responsibilities.

I understand and acknowledge that should I become aware of any misuse of information or information systems, I am obligated to inform a member of management immediately.

I understand and acknowledge that the Company reserves the right to monitor system activity and usage, including Internet activity. My signature on this document means I have consented to this monitoring.

I understand and acknowledge that there should be no expectation of privacy or ownership. All emails, files, and documents—including personal messages, files, and documents—created, sent, received, or stored on information systems or devices that are owned, leased, administered, or otherwise under the custody and control of the Company are the property of the Company and may be subject to review.

I further understand and acknowledge that violation of this policy may result in disciplinary action. Depending on the severity or frequency of the violations, this could include:

1. Counseling statements for policy violations.
2. A suspension or termination of access permissions, which could result in a job reassignment and compensation modification.
3. A termination of employment.
4. Personal liability under applicable local, state, or international laws.

Acknowledged and agreed to by: ______________________________________

Information Systems User Signature Date

Name (Printed) ____

Please complete and send this form to HR.

Acceptable Use of Information Systems Policy

1.0 Data Protection

1.1. Access to information systems is restricted to authorized users with a need-to-know.

1.2. Information systems users must utilize Company systems and devices solely for the purposes for which they were granted access.

1.3. All information systems users are expressly forbidden from accessing, or from attempting to access, any data or programs for which they do not have authorization or explicit consent.

1.4. In the event that an information systems user is sent or inadvertently accesses files that contain information that the user does not have a "need to know," or authority to receive, the user is required to immediately secure the material from view and notify their supervisor.

1.5. Customer-related files are classified as "protected." Please refer to the Data Handling Requirements Matrix for instructions on working with "protected" data.

1.6. Company-related files are classified as "confidential." Please refer to the Data Handling Requirements Matrix for instructions on working with "confidential" data.

1.7. Information systems users are forbidden from making copies of any data from any Company information system or device unless approved by management.

1.8. Data may not be removed, transported, or transmitted from the Company without the specific and expressed approval of the Information Security Officer. If approved, only storage media and transmission technology provided by the Company may be used.

1.9. Pictures or videos of information systems, data, facilities, or other workforce personnel may not be taken without the specific and expressed permission of the Information Security Officer.

2.0 Authentication and Password Controls

2.1. Information systems users are required to log in using their assigned username and password regardless of the workstation or device being used. Every user is responsible for any and all actions performed that are associated with their network or application account.

2.2. It is important to protect login credentials from disclosure. Users must not share or disclose their user account(s), passwords, personal identification numbers (PINs), security tokens, or similar information or devices used for identification and authorization purposes.

2.3. Users must not circumvent password entry with auto-login, application remembering, embedded scripts, or hard-coded passwords in client software.

2.4. Users must not use any Company password for personal applications, including email and social media accounts.

2.5. Users must report all password compromises or attempted compromises to the Help Desk.

2.6. Network, Company application, mobile device, and Internet passwords must meet or exceed the following criteria:

- Passwords must be at least eight characters long and must be composed of a minimum of three out of the following four types of characters: numbers, lowercase letters, uppercase letters, and special characters (such as, #, &, *, and so on).
- The password must not include the user's first or last name, and should not contain obvious words or names such as those of children, pets, or favorite hobbies.
- Passwords must be changed at least every 90 days.
- Users are not permitted to reuse any of their last ten passwords when selecting a new password.

2.7. Computing devices must not be left unattended without enabling a password protected screen-saver, locking the workstation, or completely logging off of the device.

3.0 Application Security

3.1. Only applications that are legally licensed to the Company may be installed on any of the Company computer systems or devices. If trial software is installed, it must be uninstalled after the trial period has expired unless a full-use license is purchased.

3.2. Before an application can be installed on any of the Company systems, the application must be evaluated and approved by the Information Security Officer or designee to ensure that it meets minimum security requirements.

3.3. Applications must be able to support access privileges adequate for the classification level of the information being handled.

3.4. Applications, upgrades, and enhancements to be installed on information systems must follow the Company change control process.

3.5. Information systems users must not make unauthorized copies of copyrighted software.

4.0 Messaging Use and Security

4.1. For the purpose of this policy, the term "messaging" applies broadly to email messages, text messages, BlackBerry messages, iPhone/iPad messages, and all similar technologies.

4.2. All messages are the property of the Company. The Company has the right, with or without cause, to review, examine, archive, retrieve, restore, investigate, and delete all messages.

4.3. Regular (non-secure) messaging should *never* be used to send or transmit customer data outside of the Company. Customer information can be sent via encrypted email. To do so, include the word "secure" in the subject line.

4.4. Customer-related messages must not be forwarded under any circumstances to personal accounts.

4.5. Information systems users must not open attachments that arrive from an unknown or unrecognizable source.

4.6. Access to personal email accounts (such as Yahoo!, Google, Hotmail, and so on) from inside the Company network is not allowed.

4.7. Anonymous or disguised e-messages are prohibited under all circumstances, as are bulk emails ("spam") and chain letters.

4.8. Company messaging systems are not to be used for the transmission of funding solicitations, requests for donations, and so on, whether initiated by the information systems user or forwarded from another source.

5.0 Internet Use and Security

5.1. Internet access from Company premises is for business purposes. Personal use is at the discretion of departmental management.

5.2. Internet access is subject to filtering at the discretion of the Company.

5.3. Access to social media sites such as Twitter and Facebook is allowed only for those information systems users that have an approved business need.

5.4. Internet access is monitored.

5.5. Information systems users must not download software, shareware, or freeware from any Internet site with the expressed permission of an information technology department employee.

5.6. Information systems users must not knowingly visit Internet sites that contain obscene, hateful, or other objectionable materials; send or receive any material, whether by email, voice mail, memoranda, or oral conversation, that is obscene, defamatory, harassing, intimidating, offensive, discriminatory, or that is intended to annoy, harass, or intimidate another person.

5.7. Information systems users must not knowingly violate copyrights or intellectual property laws.

5.8. Informations systems users must not knowingly engage in activities that violate local, state, or federal laws.

6.0 Mobile Devices Security

6.1. Mobile device users are subject to all Acceptable Use requirements contained herein.

6.2. Only approved mobile devices may be used to access Company information resources.

6.3. Mobile device use must be authorized by the Director of Information Technology.

6.4. Mobile device users will be required to acknowledge and sign a Mobile Device Agreement.

6.5. All mobile devices must be encrypted.

6.6. Mobile device passwords must conform to the password requirements detailed in Section 2.6 of this policy.

6.7. Mobile devices will be configured to be wiped after five failed password attempts.

6.8. Mobile devices will be configured with screen savers that lock after ten minutes of inactivity.

6.9. Mobile device users are responsible for ensuring the devices are secured and properly stored at all times.

6.10. Lost or stolen portable devices must be reported to the Help Desk immediately.

6.11. Mobile devices must be returned to the Company during periods of extended absence, upon termination, or upon request of management.

7.0 Remote Access Security

7.1. Remote access users are subject to all Acceptable Use requirements contained herein.

7.2. Remote access users must be authorized by the Information Security Officer.

7.3. Remote access users will be required to acknowledge and sign a Remote Access Agreement.

7.4. Only Company-owned equipment may be used for remote access connections.

7.5. All remote access sessions require multifactor authentication.

7.6. Split tunneling is not allowed. All traffic during remote sessions must be directed through the corporate network.

7.7. Remote access sessions will be automatically disconnected after one minute of inactivity.

8.0 Incident Detection and Reporting

8.1. Information systems users should immediately notify their supervisor or the Information Security Officer if there is any suspicion or cause for concern about the safety and security of customer or Company information or information systems.

8.2. In the event malware is suspected:

- Immediately contact the Help Desk.
- Do not continue to use the device.
- Do not turn off the device.
- Make no attempt to remove the malware.

Index

PEARSON   ALWAYS LEARNING

PEARSON IT CERTIFICATION

Browse by Exams ▾ | Browse by Technology ▾ | Browse by Format | Explore ▾ | I'm New Here – Help!

Store | Forums | Safari Books Online

Pearson IT Certification

THE LEADER IN IT CERTIFICATION LEARNING TOOLS

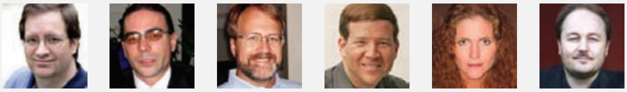
Visit pearsonITcertification.com today to find:

- IT CERTIFICATION EXAM information and guidance for

  CISCO   CompTIA   Microsoft   vmware

  Pearson is the official publisher of Cisco Press, IBM Press, VMware Press and is a Platinum CompTIA Publishing Partner—CompTIA's highest partnership accreditation

- EXAM TIPS AND TRICKS from Pearson IT Certification's expert authors and industry experts, such as
  - *Mark Edward Soper* – CompTIA
  - *David Prowse* – CompTIA
  - *Wendell Odom* – Cisco
  - *Kevin Wallace* – Cisco and CompTIA
  - *Shon Harris* – Security
  - *Thomas Erl* – SOACP



- SPECIAL OFFERS – pearsonITcertification.com/promotions

- REGISTER your Pearson IT Certification products to access additional online material and receive a coupon to be used on your next purchase

Articles & Chapters

Blogs

Books

Cert Flash Cards Online

eBooks

Mobile Apps

Newsletters

Podcasts

Question of the Day

Rough Cuts

Short Cuts

Software Downloads

Videos

CONNECT WITH PEARSON IT CERTIFICATION

Be sure to create an account on pearsonITcertification.com and receive members-only offers and benefits