Ch.3 summary By @MHazazi

CIA

- CIA stands for: Confidentiality, Integrity, and Availability.
- Collectively referred to as the CIA triad or CIA security model.
- Each attribute represents a fundamental objective of information security.
- Attack against elements of CIA triad is an attack against Information Security of the organization.
- **information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Protecting the CIA triad means protecting the assets of the company

تعاريف مختصرة

Integrity

Protecting data, processes, systems from intentional or accidental unauthorized modification.

Confidentiality

confidential information not be disclosed to unauthorized individuals.

Availability

assurance that systems and data are accessible by authorized users when needed

What Is Confidentiality?

- confidential information not be disclosed to unauthorized individuals
- Not all data owned by the company should be made available to the public
- Failing to protect data confidentiality can be disastrous for an organization (health , banking info)
- Only authorized users should gain access to information
- Information must be protected when it is used, shared, transmitted, and stored
- Information must be protected from unauthorized users internally and externally
- Information must be protected whether it is in digital or paper format

- **The threats to confidentiality must be identified. They include:**
  - Hackers and hacktivists
  - Shoulder surfing
  - Lack of shredding of paper documents
  - Malicious Code (Virus, worms, Trojans)
  - Unauthorized employee activity
  - Improper access control

What Is Integrity?

- Protecting data, processes, systems from intentional or accidental unauthorized modification.
  - ***Data integrity*** information existing as it was intended to be.
  - ***System integrity*** system function and operate as it was intended to be.

- A business that cannot trust the integrity of its data is a business that cannot operate
- An attack against data integrity can mean the end of an organization's capability to do business

- **Threats to data integrity include:**
  - Human error
  - Hackers
  - Unauthorized user activity
  - Improper access control
  - Malicious code
  - Man in the middle interception and modification

- **Controls that can be deployed to protect data integrity include:**
  1. **Access controls:**
     - Encryption
     - Digital signatures
  2. **Process controls**
     - Code testing
  3. **Monitoring controls**
     - File integrity monitoring
     - Log analysis
  4. **Behavioral controls:**
     - Separation of duties
     - Rotation of duties
     - End user security training

What Is Availability?

- assurance that systems and data are accessible by authorized users when needed
- A risk assessment should be conducted to more efficiently protect data availability
- **Threats to data availability include:**
  - Natural disaster
  - Hardware failures
  - Programming errors
  - Human errors
  - DDoS
  - Loss of power
  - Malicious code
  - Temporary or permanent loss of key personnel

The Five A's of Information Security

- Used to support CIA

Accountability	- All actions should be traceable to the person who committed them - Logs should be kept, archived, and secured - Intrusion detection systems should be deployed - Computer forensic techniques can be used in cyber crime investigation - Accountability should be focused on internal and external actions
Assurance	- Security measures need to be designed and tested to insure they are efficient - The knowledge that these measures are efficient is known as assurance - The activities related to assurance include: • Auditing and monitoring • Testing • Reporting
Authentication	- It is the positive identification of the person/system requesting access to secured information/system. - Example: • User ID and password combination • Tokens • Biometric devices
Authorization	- Act of granting users/systems actual permission to information resources. - permission level may change based on the user's defined access level - Examples : Read only , Read and write , Full

Accounting	- logging of access and usage of resources - Keeps track of who accesses what resource, when, and for how long - Example: Internet café, users are charged by the minute of use of the service

Who Is Responsible for CIA?

- **Information owner**
  - An official with permitted or operational authority for specified information
  - Ensure information is protected from creation to destruction
- **Information custodian**
  - Maintain the systems that store, process, and transmit the information

Information Security Framework

NIST= Information Technology and Security Framework by

ISO = Information Security Management System