WEEK 6| Chapter 6: Human Resources Security

Objectives

- 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

الأهداف

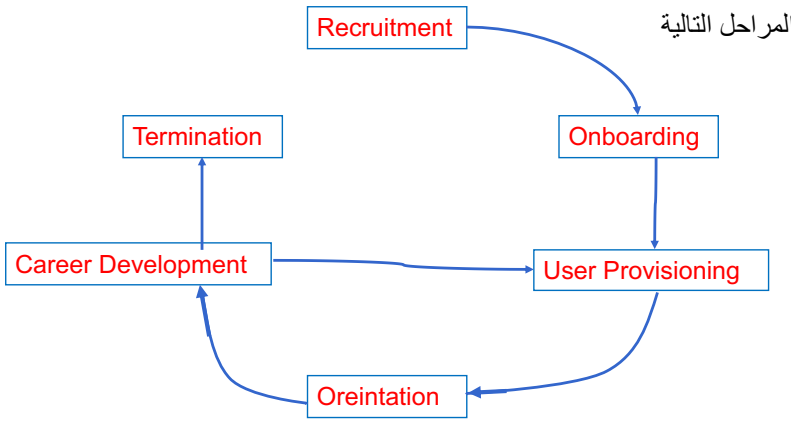
- تحديد العلاقة بين أمن المعلومات وممارسات الموظفين
- التعرف على مراحل دورة حياة الموظف
- وصف الغرض من السرية واتفاقات الاستخدام المقبول
- فهم برامج التثقيف والتدريب والتوعية الأمنية المناسبة
- إنشاء سياسات وإجراءات أمنية متعلقة بالموظفين

The Employee Lifecycle

- Represents stages in the employee's career
- Lifecycle models can vary but most include the following stages
  - Recruitment
  - Onboarding
  - User provisioning
  - Orientation
  - Career development
  - Termination

دورة حياة الموظف

- يمثل مراحل في مهنة الموظف
- قد تختلف نماذج دورة الحياة ، ولكن معظمها يتضمن المراحل التالية
  - التوظيف
  - الإعداد
  - تزويد المستخدم
  - التوجيه
  - التطوير الوظيفي
  - انهاء العمل



The Employee Lifecycle (Cont.)

- Recruitment— It includes all the processes leading up to and including the hiring of a new employee.
- Onboarding— The employee is added to the organization's payroll and benefits systems.
- User provisioning— The employee is assigned equipment as well as physical and technical access permissions.
  - It is also invoked whenever there is a change in the employee's position, level of access required, or termination.
- Orientation— 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— The employee matures in his role in the organization. Professional development frequently means a change in roles and responsibilities.
- Termination— The employee leaves the organization.
  - 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.

دورة حياة الموظف

- التوظيف - يشمل جميع العمليات التي تؤدي إلى توظيف موظف جديد.
- Onboarding - يتم إضافة الموظف إلى نظام الرواتب والمزايا الخاص بالمنظمة.
- إدارة حسابات المستخدم - يتم تعيين الموظف والمعدات وكذلك أذونات الوصول المادية والفنية.
  - يتم استدعاؤه أيضًا عند حدوث تغيير في وضع الموظف أو مستوى الوصول المطلوب أو الإنهاء.
- التوجيه - يستقر الموظف في الوظيفة ، ويتكامل مع ثقافة الشركة ، ويعرف نفسه مع زملاء العمل والإدارة ، ويؤسس دوره داخل المنظمة.
- التطوير الوظيفي - ينضج الموظف في دوره في المنظمة. التطوير المهني يعني في كثير من الأحيان تغيير في الأدوار والمسؤوليات.
- الإنهاء - يترك الموظف المؤسسة.
  - تعتمد العمليات إلى حد ما على ما إذا كان الرحيل ناتجًا عن الاستقالة أو التقاعد. تشمل المهام إزالة الموظف من نظام الرواتب والمزايا ، واسترداد أصول المعلومات مثل هاتفه الذكي ، وحذف أو تعطيل حسابات المستخدمين وأذونات الوصول.

What Does Recruitment Have to Do with Security?

Risks and rewards of posting online employment ads:

- A company can reach a wider audience
- A company can publish an ad that gives too much information:
  - About the network infrastructure and therefore allow a hacker to footprint the internal network easily and stealthily
  - About the company itself, inviting social engineering attacks

ماذا يجب على التوظيف أن يفعل مع الأمن؟

المخاطر والمزايا لنشر إعلانات التوظيف عبر الإنترنت:

- يمكن للشركة الوصول إلى جمهور أوسع
- يمكن للشركة أن تنشر إعلانًا يعطي الكثير من المعلومات:
  - حول البنية التحتية للشبكة ، وبالتالي تسمح للهاكر بالدخول للشبكة الداخلية بسهولة وخلسة
  - حول الشركة نفسها ، ودعوة لهجمات الهندسة الاجتماعية

Job Postings

- Job descriptions are supposed to:
  - Convey the mission of the organization
  - Describe the position in general terms
  - Outline the responsibilities attached to said position
  - Outline the company's commitment to security via the use of such terms as non-disclosure agreement
- Job descriptions are NOT supposed to:
  - Include information about specific systems, software versions, security configurations, or access controls
    - It's harder to hack a network if one doesn't know what hardware & software
  - If the above information is deemed necessary, two versions of the position can be created. The second, more detailed version should be posted internally and shared with candidates that have made the "first cut"

وظائف شاغرة

- من المفترض أن الوصف الوظيفي هو:
  - نقل مهمة المنظمة
  - وصف الموقف بشكل عام
  - الخطوط العريضة للمسؤوليات المرتبطة بهذا المنصب
  - تحديد التزام الشركة بالأمان من خلال استخدام مصطلحات مثل اتفاقية عدم الإفشاء
- لا يُفترض أن تتضمن الأوصاف الوظيفية ما يلي:
  - تضمين معلومات حول أنظمة معينة أو إصدارات البرامج أو تكوينات الأمان أو عناصر التحكم في الوصول
  - من الصعب اختراق شبكة إذا لم يكن أحد يعرف الأجهزة والبرامج
  - إذا اعتبرت المعلومات المذكورة أعلاه ضرورية ، فيمكن إنشاء نسختين من الموضع. يجب نشر النسخة الثانية الأكثر تفصيلاً داخليًا ومشاركتها مع المرشحين الذين لديهم "أول خطوة من نوعها"

Candidate Application Data

- Companies are responsible for protecting the data and privacy of the job seeker
- Non-public personal information (NPPI) should not be collected if possible

بيانات طلب المرشح

- الشركات مسؤولة عن حماية بيانات وخصوصية الباحث عن العمل
- لا ينبغي جمع المعلومات الشخصية غير العامة (NPPI) إن أمكن

The Interview

Job Interview:

- The interviewer should be concerned about revealing too much about the company during the interview
- Job candidates should never gain access to secured areas
- A job interview is a perfect foot-printing opportunity for hackers and social engineers

المقابلة

مقابلة عمل:

- ينبغي على القائم بإجراء المقابلة أن يهتم بشأن الكشف عن الكثير عن الشركة خلال المقابلة
- يجب ألا يحصل المرشحون للوظائف الوصول إلى المناطق الآمنة
- مقابلة العمل هي فرصة مثالية للقراصنة والمهندسين الاجتماعيين

Screening Prospective Employees

- An organization should protect itself by running extensive background checks on potential employees at all levels of the hierarchy
- Some higher level positions may require even more in-depth checks
- Many U.S. government jobs require prospective employees have the requisite clearance level

تسليط الضوء الموظفين المحتملين

- يجب على المؤسسة أن تحمي نفسها من خلال إجراء بحث مكثف على خلفية الموظفين المحتملين على جميع مستويات التسلسل الهرمي
- قد تتطلب بعض المراكز الأعلى مستوى مزيدًا من البحث المتعمق
- تتطلب العديد من الوظائف الحكومية في U.S أن يكون لدى الموظفين المحتملين كشف حسابات توضح

Types of Background Checks

- The company should have a basic background check level to which all employees are subjected
- Information owners may require more in-depth checks for specific roles
- **Workers also have a right to privacy:** Not all information is fair game to gather – only information relevant to the actual work they perform
- Companies should seek **consent** from employees before launching a background check
- Using social media – to learn more about the candidate. – but law prohibits the act of checking the gender, religion, race for the purpose of recruitment
- Educational records fall under FERPA(Family Educational Rights and Privacy Act). Schools must first have written authorization before they can provide student-related information
- Motor vehicle records fall under DPPA(Drivers Privacy Protection Act), which means that the DMV – or its employees – are not allowed to disclose information obtained by the department
- The FTC(Federal Trade Commission) allows the use of credit reports prior to hiring employees as long as companies do so in accordance with the Fair Credit Reporting Act
- Bankruptcies may not be used as the SOLE reason to not hire someone according to Title 11 of the U.S. Bankruptcy Code
- Criminal history: The use of this sort of information varies from state to state
- Worker's compensation records: In most states, these records are public records, but their use may not violate the Americans with Disabilities Act

أنواع تحقق الخلفية

- يجب أن يكون للشركة مستوى فحص أساسي في الخلفية يخضع له جميع الموظفين
- قد يتطلب مالكو المعلومات المزيد من الفحوصات المتعمقة لأدوار محددة
- للعمال أيضًا الحق في الخصوصية: لا تعد كل المعلومات لعبة عادلة لجمعها - فقط المعلومات ذات الصلة بالعمل الفعلي الذي يقومون به
- يجب على الشركات الحصول على موافقة من الموظفين قبل عمل بحث حول خلفيتهم
- استخدام وسائل الإعلام الاجتماعية - لمعرفة المزيد عن المرشح. - لكن القانون يحظر فعل التحقق من الجنس أو الدين أو العرق لغرض التوظيف

- السجلات التعليمية تندرج تحت FERPA (قانون الخصوصية والحقوق التعليمية للأسرة). يجب أن تحصل المدارس أولاً على تفويض كتابي قبل أن تتمكن من تقديم معلومات ذات صلة بالطلاب
- تندرج سجلات السيارات تحت DPPA (قانون حماية خصوصية السائقين) ، مما يعني أن DMV - أو موظفيها - غير مسموح لهم بالإفصاح عن المعلومات التي تم الحصول عليها من الإدارة.
- يسمح FTC باستخدام تقارير الائتمان قبل توظيف الموظفين طالما أن الشركات تفعل ذلك وفقا لقانون الإبلاغ عن الائتمان العادل
- لا يجوز استخدام حالات الإفلاس باعتبارها السبب الوحيد لعدم توظيف شخص ما وفقًا للفقره 11 من قانون الإفلاس بالولايات المتحدة.
- السجل الجنائي: يختلف استخدام هذا النوع من المعلومات من ولاية إلى أخرى
- سجلات تعويض العمال: في معظم الولايات ، تعتبر هذه السجلات سجلات عامة ، ولكن استخدامها قد لا ينتهك قانون الأمريكيين ذوي الإعاقة

What Happens in the Onboarding Phase?

- The new hire is added to the organization's payroll and benefit systems
- New employees must provide
  - Proof of identity
  - Work authorization
  - Tax identification
- Two forms that must be completed
  - Form I-9-
  - Form W-4

ماذا يحدث في مرحلة الإعداد؟

- يتم إضافة الأجر الجديد إلى نظام الرواتب والمزايا الخاص بالمنظمة
- يجب على الموظفين الجدد تقديم
  - إثبات الهوية
  - تصريح عمل
  - التعريف الضريبي
- اثنين من النماذج التي يجب أن تكتمل
  - يضمن نموذج I-9
  - نموذج W-4

What Is User Provisioning?

- The process of:
  - Creating user accounts and group memberships
  - Providing company identification
  - Assigning access rights and permissions
  - Assigning access devices such as tokens and/or smartcards
- The user should be provided with and acknowledge the terms and conditions of the **Acceptable Use Agreement** before being granted access

ما هو تزويد المستخدم؟

- عملية:
  - إنشاء حسابات المستخدمين وعضوية المجموعة
  - تقديم تعريف الشركة
  - تعيين حقوق الوصول والأذونات
  - تعيين أجهزة الوصول مثل الرموز المميزة و / أو البطاقات الذكية
- يجب أن يتم تزويد المستخدم وتأكيده على بنود وشروط **اتفاقية الاستخدام المقبول** قبل منحه حق الدخول

What Should an Employee Learn During Orientation?

- His responsibilities
- Information handling standards and privacy protocols
- Ask questions

ما الذي يجب على الموظف تعلمه أثناء مرحلة التوجيه؟

- مسؤولياته
- معايير التعامل مع المعلومات وبروتوكولات الخصوصية
- يسأل اسئلة

The Importance of Employee Agreements

Confidentiality or non-disclosure agreements

- Agreement between employees and organization
- Defines what information may not be disclosed by employees
- Goal: To protect sensitive information
- Especially important in these situations:
  - When an employee is terminated or leaves
  - When a third-party contractor was employed

أهمية اتفاقيات الموظفين

اتفاقيات السرية أو عدم الإفشاء

- اتفاق بين الموظفين والتنظيم
- يعرف ما هي المعلومات التي لا يجوز الكشف عنها من قبل الموظفين
- الهدف: حماية المعلومات الحساسة
- مهم بشكل خاص في هذه المواقف:
  - عندما يتم إنهاءعمل الموظف أو يترك العمل
  - عندما يعمل طرف ثالث كمتعاقد

The Importance of Employee Agreements cont

- Acceptable Use Agreement
  - A policy contract between the company and information systems user
- Components of an Acceptable Use Agreement
  - Introduction
  - Data classifications
  - Applicable policy statement
  - Handling standards
  - Contacts
  - Sanctions for violations
  - acknowledgment

أهمية اتفاقيات الموظفين

- اتفاقية الاستخدام المقبول
  - عقد سياسة بين الشركة ومستخدم نظم المعلومات
- مكونات اتفاقية الاستخدام المقبول
  - المقدمة
  - تصنيفات البيانات
  - بيان سياسة قابل للتطبيق
  - معايير التعامل
  - الاتصال
  - العقوبات على الانتهاكات
  - اشعار بالإستلام

The Importance of Security Education and Training

Training employees

- According to NIST: “Federal agencies […] cannot protect […] information […] without ensuring that all people involved […]:
  - Understand their role and responsibilities related to the organization’s 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”
- Hackers adapt: If it is easier to use social engineering – i.e., targeting users – rather than hack a network device, that is the road they will take
- Only securing network devices and neglecting to train users on information security topics is ignoring half of the threats against the company

أهمية التعليم الأمني والتدريب

تدريب الموظفين

- ووفقًا لـ NIST: "لا تستطيع الوكالات الفيدرالية [...] حماية [...] المعلومات [...] دون ضمان أن جميع الأشخاص المشاركين [...]:
  - فهم دورهم ومسؤولياتهم المتعلقة بمهمة المنظمة
  - فهم سياسة أمان تكنولوجيا المعلومات والإجراءات والممارسات في المنظمة
  - أن يكون لديهم على الأقل معرفة كافية عن مختلف الضوابط الإدارية والتشغيلية والتقنية المطلوبة والمتاحة لحماية موارد تكنولوجيا المعلومات التي تكون مسؤولة عنها "
- تكيف القراصنة: إذا كان من الأسهل استخدام الهندسة الاجتماعية - أي استهداف المستخدمين - بدلاً من اختراق جهاز شبكة ، فهذا هو الطريق الذي سيأخذونه
- تأمين أجهزة الشبكة فقط وإهمال تدريب المستخدمين على مواضيع أمن المعلومات وتجاهل نصف التهديدات ضد الشركة

What Is the SETA Model?

- What is SETA?
  - Security Education Training and Awareness
  - Awareness is not training: It is focusing the attention of employees on security topics to change their behavior
  - Security awareness campaigns should be scheduled regularly
  - Security training “seeks to teach skills” (per NIST)
  - Security training should NOT be dispensed only to the technical staff but to all employees

ما هو نموذج SETA؟

- ما هو SETA؟
  - التعليم الأمني والتدريب والتوعية
  - التوعيه ليس تدريبًا: إنه تركيز انتباه الموظفين على موضوعات أمنية لتغيير سلوكهم
  - يجب تنظيم حملات التوعية الأمنية بانتظام
  - التدريب الأمني "يسعى لتعليم المهارات" (لكل NIST)
  - يجب ألا يتم توزيع التدريب الأمني على الموظفين الفنيين فحسب بل لجميع الموظفين

Summary

- A security policy that does not include personnel as a permanent threat to the data owned by the company is incomplete. Social engineering is more virulent than ever.
- Failing to train users on security topics is a bad mistake and may result in a lack of compliance for some federal mandates.
- All users should sign the Acceptable Use Agreement before receiving access to company’s systems and equipment

ملخص

- السياسة الأمنية التي لا تتضمن الأفراد كتهديد دائم للبيانات المملوكة للشركة غير كاملة. الهندسة الاجتماعية هي أكثر فتكا من أي وقت مضى.
- يعد عدم تدريب المستخدمين على مواضيع الأمان خطأً فادحًا وقد يؤدي إلى عدم الامتثال لبعض الولايات الفيدرالية.
- يجب على جميع المستخدمين توقيع اتفاقية الاستخدام المقبول قبل استلام الوصول إلى أنظمة ومعدات الشركة

GOOD LUCK IN MID EXAM