Ch.6 summary By @MHazazi

The Employee Lifecycle

- Represents stages in the employee's career
- **Lifecycle stages:**

  Recruitment , Onboarding , User provisioning , Orientation , Career development , Termination

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 as result hacker will footprint internal network easily
    - About the company itself, inviting social engineering attacks

Job Postings

- **Job descriptions are supposed to:**
  - Convey mission of organization
  - Describe position generally
  - Outline responsibilities attached to position
  - Outline the company's commitment to security via non-disclosure agreement
- **Job descriptions are NOT supposed to:**
  - Include information about specific systems, software versions, security configurations
  - 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

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

The Interview

- interviewer should be concerned about revealing too much about 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

Screening Prospective Employees

- An organization should protect itself by running extensive background checks about employees
- Some higher level positions may require even in-depth checks
- Many U.S. government jobs require prospective employees have the requisite clearance level

Types of Background Checks

- Basic background check level to which all employees are subjected
- in-depth checks for specific roles
- only information relevant to the actual work they perform is required.
- Company should seek consent from employees before launching a background check
- Educational records fall under FERPA. Schools must first have written authorization
- Motor vehicle records fall under DPPA, not allowed to disclose information
- FTC allows the use of credit reports prior to hiring employees
- Bankruptcies may not be used as the SOLE reason to not hire someone
- Criminal history: The use of this sort of information varies from state to state
- Worker's compensation records: public records

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

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

What Should an Employee Learn During Orientation?

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

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
- 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

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

What Is the SETA Model?

SETA = Security , Education , Training , Awareness

- Awareness is not training: 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