PEARSON IT CYBERSECURITY CURRICULUM

DEVELOPING CYBERSECURITY PROGRAMS AND POLICIES

OMAR SANTOS

Developing Cybersecurity Programs and Policies

Omar Santos

Pearson

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 use this information only 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.

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 Information Security (or Cybersecurity 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.

Obtaining a U.S. government security clearance involves a four-phase process:

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:** To obtain access to data, clearance and classification must match. For example, 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 one’s 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. 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 https://www.uscis.gov/i-9. 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, and 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 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 Cybersecurity department, or the Information Technology (IT) department.

One important step toward securing your infrastructure and effective identity management practices is to ensure that you can manage user accounts from one single location regardless of where these accounts were created. Although the majority of organizations will have their primary account directory on-premise, hybrid cloud deployments are on the rise, and it is important that you understand how to integrate on-premise and cloud directories and provide a seamless experience to the end user, and to also manage onboarding of new employees and deleting accounts for departing employees. To accomplish this hybrid identity scenario, it is recommended that you synchronize and federate your on-premise directory with your cloud directory. A practical example of this is using Active Directory Federation Services (ADFS). We discuss role-based access controls and other identity management topics 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 or Cybersecurity 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 co-workers. 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 cybersecurity 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 or Cybersecurity 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. Many organizations have painfully discovered that employees who left their company voluntarily or because of layoffs have retained access to corporate applications, and some have logged in to corporate resources after leaving the company. In a perfect world, you would like to trust everyone to do the right thing after leaving your organization, but unfortunately, that is not the case.

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 for a competitor, the best bet is to escort them off the property immediately. In all cases, make sure not to forget about remote access capabilities.

FYI: The Insider Threat

The insider threat has never been more real. Insiders have a significant advantage over external threat actors. They not only have access to internal resources and information, but they are also aware of the organization's policies, procedures, and technology (and potential gaps in those policies, procedures, and technologies). The risk of insider threats requires a different strategy from other cybersecurity challenges. This is because of their inherent nature. The Computer Emergency Response Team (CERT) Insider Threat Center at Carnegie Mellon's Software Engineering Institute (SEI) has many resources that were created to help you identify potential and realized insider threats in your organization, institute ways to prevent and detect them, and establish processes to deal with them if they do happen.

You can obtain more information about CERT's Insider Threat Center at: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91513.

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 or Cybersecurity are jointly responsible for the user provisioning process.