Necessary Skills Now

STUDENT: SECURITY POLICIES

Document Version: 2018-10-01

This material is based upon work supported by the National Science Foundation under DUE #1501990. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Contents

Overview

This project includes the following tasks:

1. Review and prioritize scenario audit observations
2. Develop an information security policy and related procedure
3. Develop an implementation and dissemination plan

Objective: Developing Information Security Policies

A security policy is the document developed by an organization that formally states how it plans to protect its information and information systems. Organizations should treat a security policy as a "living document." This means that the organization continuously reviews and updates the document as technology and employee requirements change.

Organizations use several documents to support its policy infrastructure. In this project, you will be developing the following documents:

- An information security policy
- A procedure to support the policy

An effective security policy references the standards and guidelines that exist within an organization. An information security policy contains high-level statements with the intent of protecting information and assets. It is the responsibility of senior management to develop security policies.

Standards are mandatory controls that enforce and support the information security policy. Standards are a collection of properties or rules that an organization formally adopts and recognizes. There are many standards organizations in the information technology field including IEEE, EIA/TIA, NIST and ISO.

Guidelines are recommended, nonmandatory controls that support standards and provide a foundation for the development of best practices.

Procedures are the systematic instructions used by employees within the organization that explain how to implement the controls defined in the policies, standards, and guidelines.

For example, a password policy states the standard for creating strong passwords and protecting passwords. A password construction guideline defines how to create a strong password and provides best practices recommendations. The password procedure provides the instructions on how to implement the strong password requirement. Organizations do not update policies as frequently as they update procedures within the information security policy framework.

Supplemental Materials

a. Information Security Policy — A Development Guide
b. Technical Writing for IT Security Policies in Five Easy Steps

Website Links

a. Information Security Policy Templates
b. Information Security Policy (video)

Project Scenario

ACME Healthcare is a healthcare company that runs over 25 medical facilities including patient care, diagnostics, outpatient care, and emergency care. The organization has experienced several data breaches over the last five years. These data breaches have cost the organization financially and damaged its reputation.

The executive leadership team recently hired a new chief information security officer (CISO). The new CISO has brought in one of the top cybersecurity penetration teams to perform a full security audit on the entire organization. This independent contractor conducted the audit, and found the following vulnerabilities:

1. Several accounts were identified for employees that are no longer employed by ACME.
2. Several user accounts allowed unauthorized and escalated privileges and accessed systems and information without formal authorization.
3. Several devices and systems allowed unsecure remote access.
4. Forty percent of all organization passwords audited were cracked within 6 hours.
5. Password expiration was not standardized.
6. Sensitive files were found unencrypted on user systems and laptops.
7. Several wireless hotspots used WEP for encryption and authentication.
8. Evidence indicates that sensitive e-mail was sent unencrypted to and from employee homes and mobile devices.
9. Intrusion detection logs were infrequently reviewed and analyzed.
10. Systems with sensitive company data were used by employees for private use.
11. Employee systems were left unattended and employees failed to logout of the company network and data systems.
12. Inconsistent system updates and configurations were performed.
13. Several firewall rules were set to permit all traffic unless specifically denied.
14. Company servers were not updated with the latest patches.
15. Intranet web server allowed users to change personal information about themselves, including contact information (address, phone number, etc.).

1 Overview the Scenario

1. Read over the scenario given above. As a class, watch the ***Information Security Policy*** video. Take notes to help you differentiate the various levels and types of policies.

2 Review and Prioritize Audit Findings

1. As directed by the instructor, form groups of 3 to 5 students. Review the security audit findings from the scenario with your group members.
2. Research the types of vulnerabilities listed to determine which pose the greatest threat.
3. Based on your group's research, agree on the top five security audit findings that ACME should address, starting with the greatest vulnerability.
4. Record your rankings in a **Vulnerabilities Ranking Table,** like shown below, that lists the a) *Vulnerabilities*, b) the *Recommended Policy* to mitigate this vulnerability, and c) your *Justification*.

Vulnerabilities Ranking Table		
Vulnerability	**Recommended Policy**	**Justification**

3 Develop Policy Documents

3.1 Create an Information Security Policy

1. As a team, assign each member a vulnerability in the table for which to develop a security policy.
2. Use the SANS templates (see Weblinks above) to develop a specific security policy for ACME Healthcare that addresses your assigned vulnerability.

NOTE: Follow the template as a guideline. Address all existing policy elements. No policy should exceed two pages in length.

3.2 Create a Procedure

1. Create a step-by-step set of instructions that supports your information security policy.
2. Include all of the information that a user would need to properly configure or complete the task in accordance with the security policy.

4 Develop Plan to Disseminate and Evaluate Policies

As a team, discuss and document information required to create an information security policy implementation and dissemination plan. Include specific tasks and events that ACME Healthcare will use to make sure that all employees involved are aware of the information security policies that pertain to them. The plan should include any specific departments that need to be involved. ACME Healthcare must also be able to assess whether individuals have the proper knowledge of the policies that pertain to their job responsibilities.

5 Optional: Prepare and Deliver a Presentation to ACME Managers

For each of the policies developed by your team, one team member should prepare a 3- to 5-minute presentation, as if to a room of ACME managers, to present 1) the case for needing a new policy and 2) the proposed policy, including 3) cost estimates, both with and without the policies, and 4) other evidence to support the recommendation for the new policy. **Hint:** Practice your presentation with your team, and listen to their suggestions for improvement before delivery to the ACME Managers.

Conclusion

Information security policies provide a framework for how an organization protects its assets and is a safeguard that the organization employs to reduce risk. This project examined **why** an organization develops information security policies, and the **differences** between information security policies, standards, guidelines, and procedures. This project also explored how an organization disseminates and evaluates information security policies.