Information Security Maintenance

Learning Objectives

At the end of this learning activity, you should be able to:

1. Understand why maintenance of the information security program is needed on an ongoing basis.
2. Recognize recommended security management models.
3. Define a model for a full maintenance program.
4. Identify the key factors involved in monitoring the external and internal environment.
5. Understand how planning and risk assessment tie into information security maintenance.
6. Understand how vulnerability assessment and remediation tie into information security maintenance.
7. Understand how to build readiness and review procedures into information security maintenance.

What should organizations do after successfully implementing and testing a new and improved information security profile?

The ISO Network Management Model

The ISO Network Management Model

- A five-layer approach that provides structure to the administration and management of networks and systems.
- Addresses management and operation through five areas: fault management, configuration, and name management; accounting management; performance management; and security management.

The ISO Network Management Model

Five areas of the ISO model transformed into five areas of security management:

I. Fault management

II. Configuration and change management

III. Accounting and auditing management

IV. Performance management

V. Security program management

The ISO Network Management Model

Five areas of the ISO model transformed into five areas of security management:

I. Fault management

- Identifying, tracking, diagnosing, and resolving faults in the system
- Vulnerability assessment is most often accomplished with penetration testing (simulated attacks exploiting documented vulnerabilities)
- Another aspect is the monitoring and resolution of user complaints
- Help desk personnel must be trained to recognize security problems as distinct from other system problems

The ISO Network Management Model

Five areas of the ISO model transformed into five areas of security management:

II. Configuration and Change Management

- Configuration management: administration of the configuration of security program components
- Change management: administration of changes in strategy, operation, or components
- Each involves non-technical as well as technical changes:
  - A. Non-technical changes impact procedures and people
  - B. Technical changes impact the technology implemented to support security efforts in the hardware, software, and data components

The ISO Network Management Model

Five areas of the ISO model transformed into five areas of security management:

II. Configuration and Change Management

A. Nontechnical Change Management

- Changes to information security may require implementing new policies and procedures
- Document manager should maintain a master copy of each document, record and archive revisions made, and keep copies of revisions
- Policy revisions are not implemented and enforceable until they have been disseminated, read, understood, and agreed to
- Software available to make creation, modification, dissemination, and agreement documentation processes more manageable

The ISO Network Management Model

Five areas of the ISO model transformed into five areas of security management:

II. Configuration and Change Management

B. Technical Configuration and Change Management

- Terms associated with the management of technical configuration and change: configuration item, version, build
- Four steps that are associated with configuration management
  - Configuration identification
  - Configuration control
  - Configuration status accounting
  - Configuration audit

The ISO Network Management Model

Five areas of the ISO model transformed into five areas of security management:

III. Accounting and Auditing Management

- Chargeback accounting enables organizations to internally charge for system use.
- Some resource usage is commonly tracked
- Accounting management involves monitoring the use of a particular component of a system.
- Auditing is the process of reviewing the use of a system, not to check performance, but to determine misuse or malfeasance; automated tools can assist.

The ISO Network Management Model

Five areas of the ISO model transformed into five areas of security management:

IV. Performance Management

- Important to monitor the performance of security systems and the underlying IT infrastructure to determine if they are working effectively
- Common metrics are applicable in security, especially when components being managed are associated with network traffic
- To evaluate the ongoing performance of the security system, performance baselines are established

The ISO Network Management Model

Five areas of the ISO model transformed into five areas of security management:

V. Security Program Management

- The ISO five-area-based framework supports a structured management model by ensuring that various areas are addressed
- Two standards are designed to assist in this effort.
- Part 2 of the British Standard (BS) 7799 introduces the process model: plan, do, check, and act.

The ISO Network Management Model

NIST Security Model

- This refers to “The National Security Telecommunications and Information Systems Security Committee” document.
- This document presents a comprehensive model for information security.
- The model consists of three dimensions..

The ISO Network Management Model

The following NIST documents can assist in the design of a security framework:

- NIST SP 800-12: An Introduction to Computer Security: The NIST Handbook
- NIST SP 800-14: Generally Accepted Security Principles and Practices for Securing IT Systems
- NIST SP 800-18: The Guide for Developing Security Plans for IT Systems
- NIST SP 800-26: Security Self-Assessment Guide for IT Systems
- NIST SP 800-30: Risk Management for IT Systems

The ISO Network Management Model

NIST Special Publication SP 800-14

- SP 800-12 is an excellent reference and guide for the security manager or administrator in the routine management of information security.
- It provides little guidance, however, on the design and implementation of new security systems, and therefore should be used only as a valuable precursor to understanding an information security blueprint.

Learning Activity # 1

1. **Explain the importance of cryptography in modern communication**. In your answer, include how cryptography supports confidentiality, integrity, and secure communication in digital environments.
2. **Differentiate between symmetric and asymmetric key cryptography**. Use practical examples (such as Alice and Bob scenarios) to illustrate how each encryption method works.
3. **Discuss the role of hashing in data security**. Provide an example of how a hashing algorithm like SHA-256 ensures the integrity of a user's password.
4. **Compare the characteristics and uses of DES, AES, and Blowfish encryption algorithms**. Highlight their key sizes, speed, and current relevance in secure communications.
5. **What is a digital signature, and how does it ensure non-repudiation?** Include in your explanation how public-key cryptography is used in this context.

Homework # 1

1. Choose one of the following cryptographic algorithms:
   - SHA-1 (Secure Hash Algorithm 1)
   - MD5 (Message Digest 5)
   - DES (Data Encryption Standard)

2. Find a sample code written in either Java or Python that demonstrates the use of your chosen algorithm. You may:
   - Search for open-source code on GitHub, tutorial sites, or documentation.
   - Write your own simple implementation (optional for bonus points).

3. Copy the code into your document or attach it as a separate file. Be sure to:
   - Add brief comments to explain each step of the code (either your own or the one you found).
   - Highlight which part is performing encryption, decryption, or hashing.

4. Answer the following questions below the code:

   a) What does this code do?

   b) What inputs are required and what outputs does it produce?

   c) Why is this algorithm considered important in cryptography?

   d) Are there any security concerns or limitations with this algorithm?

6. Cite your sources if you used any website, book, or article.