Information and Network Security

Notes

Planning for Security

Learning Objectives:

Upon completion of this chapter you should be able to:

- Understand management's responsibilities and role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
- Understand the differences between the organization's general information security policy and the requirements and objectives of the various issue-specific and system-specific policies.
- Know what an information security blueprint is and what its major components are.
- Understand how an organization institutionalizes its policies, standards, and practices using education, training, and awareness programs.
- Become familiar with what viable information security architecture is, what it includes, and how it is used.
- Explain what contingency planning is and how incident response planning, disaster recovery planning, and business continuity plans are related to contingency planning.

Introduction

- The creation of an information security program begins with the creation and/or review of the organization's information security policies, standards, and practices.
- Then, the selection or creation of information security architecture and the development and use of a detailed information security blueprint will create the plan for future success.
- This blueprint for the organization's information security efforts can be realized only if it operates in conjunction with the organization's information security policy.
- Without policy, blueprints, and planning, the organization will be unable to meet the information security needs of the various communities of interest.
- The organizations should undertake at least some planning: strategic planning to manage the allocation of resources, and contingency planning to prepare for the uncertainties of the business environment.

Information Security Policy, Standards, and Practices

- Management from all communities of interest must consider policies as the basis for all information security efforts like planning, design and deployment.
- Policies direct how issues should be addressed and technologies used
- Policies do not specify the proper operation of equipments or software-this information should be placed in the standards, procedures and practices of user's manuals and systems documentation.
- Security policies are the least expensive control to execute, but the most difficult to implement properly.
- Shaping policy is difficult because:
  - Never conflict with laws
  - Stand up in court, if challenged
  - Be properly administered through dissemination and documented acceptance.

Definitions

- A policy is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters
  A policy is a plan or course of action used by an organization to convey instructions from its senior-most management to those who make decisions, take actions, and perform other duties on behalf of the organization.
- Policies are organizational laws. Policies must define what is right, what is wrong, what the penalties for violating policy, and what the appeal process is..
- Standards, on the other hand, are more detailed statements of what must be done to comply with policy.
- Standards may be published, scrutinized, and ratified by a group, as in formal or de jury standards.
- Practices, procedures, and guidelines effectively explain how to comply with policy.
- For a policy to be effective it must be properly disseminated, read, understood and agreed to by all members of the organization
- Finally, practices, procedures, and guidelines effectively explain how to comply with policy.

- Fig 6-1 shows policies as the force that drives standards, which in turn drive practices, procedures, and guidelines.

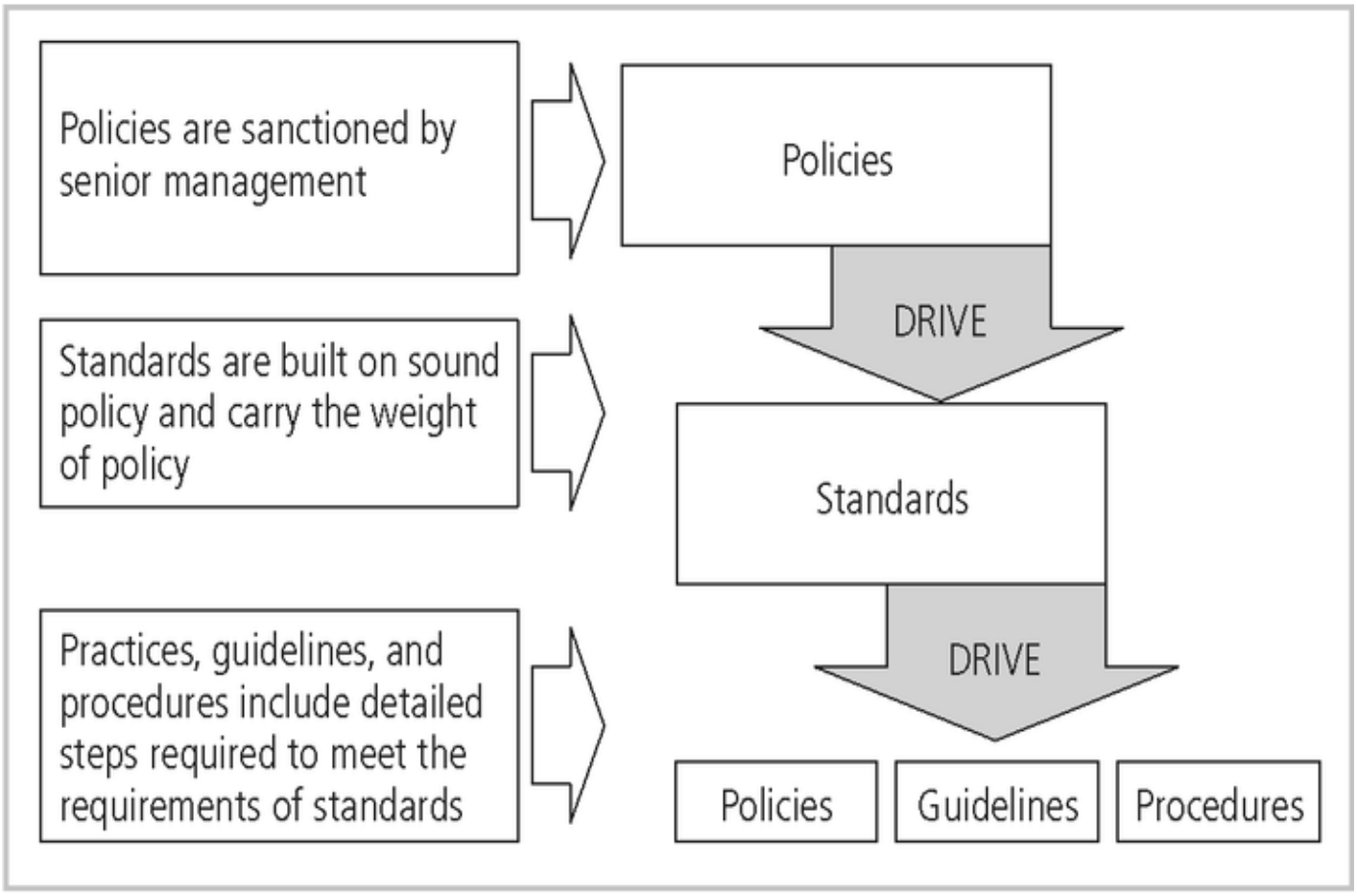

FIGURE 6-1 Policies, Standards, and Practices

- Policies are written to support the mission, vision and strategic planning of an organization.
- The MISSION of an organization is a written statement of an organization's purpose.
- The VISION of an organization is a written statement about the organization's goals-where will the organization be in five years? In ten?
- Strategic planning is the process of moving the organization towards its vision.
- A policy must be disseminated by all means possible, including printed personal manuals, organization intranets, and periodic supplements.

- All members of the organization must read, understand, and agree to the policies.
- Policies should be considered as the living documents.
- Government agencies discuss policy in terms of national security and national policies to deal with foreign states.
- A security policy can also represent a credit card agency's policy for processing credit card numbers.
- In general, a security policy is a set of rules that protect an organization's assets.
- An information security policy provides rules for the protection of the information assets of the organization.
- The task of information security professionals is to protect the confidentiality, integrity and availability of information and information systems whether in the state of transmission, storage, or processing.
- This is accomplished by applying policy, education and training programs, and technology.

Types of Policy

Management must define three types of security policy according to the National Institute of Standards and Technology's special publication 800-14.

- General or security program policies.
- Issue-specific security policies
- Systems-specific security policies.

General or Security Program Policy Enterprise Information Security Policy (EISP)

A security program policy (SPP) or EISP is also known as

- A general security policy
- IT security policy
- Information security policy

EISP

- The EISP is based on and directly supports the mission, vision, and direction of the organization and Sets the strategic direction, scope, and tone for all security efforts within the organization
- The EISP is an executive-level document, usually drafted by or with, the Chief Information Officer (CIO) of the organization and is usually 2 to 10 pages long.
- The EISP does not usually require continuous modification, unless there is a change in the strategic direction of the organization.
- The EISP guides the development, implementation, and management of the security program. It contains the requirements to be met by the information security blueprint or framework.
- It defines then purpose, scope, constraints, and applicability of the security program in the organization.
- It also assigns responsibilities for the various areas of security, including systems administration, maintenance of the information security policies, and the practices and responsibilities of the users.
- Finally, it addresses legal compliance.
- According to NIST, the EISP typically addresses compliance in two areas:
  - General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components and
  - The use of specified penalties and disciplinary action.

Issue-Specific Security Policy (ISSP)

- As various technologies and processes are implemented, certain guidelines are needed to use them properly
- The ISSP:
  - addresses specific areas of technology like
    - Electronic mail
    - Use of the Internet

- Specific minimum configurations of computers to defend against worms and viruses.
- Prohibitions against hacking or testing organization security controls.
- Home use of company-owned computer equipment.
- Use of personal equipment on company networks
- Use of telecommunications technologies (FAX and Phone)
- Use of photocopy equipment.

    - requires frequent updates
    - contains an issue statement on the organization's position on an issue

- There are a number of approaches to take when creating and managing ISSPs within an organization.
- Three approaches:
    - Independent ISSP documents, each tailored to a specific issue.
    - A single comprehensive ISSP document covering all issues.
    - A modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements.

- The independent document approach to take when creating and managing ISSPs typically has a scattershot effect.
- Each department responsible for a particular application of technology creates a policy governing its use, management, and control.
- This approach to creating ISSPs may fail to cover all of the necessary issues, and can lead to poor policy distribution, management, and enforcement.

- The single comprehensive policy approach is centrally managed and controlled.
- With formal procedures for the management of ISSPs in place , the comprehensive policy approach establishes guidelines for overall coverage of necessary issues and clearly identifies processes for the dissemination, enforcement, and review of these guidelines.
- Usually, these policies are developed by those responsible for managing the information technology resources.

- The optimal balance between the independent and comprehensive ISSP approaches is the modular approach.

- It is also certainly managed and controlled but tailored to the individual technology issues.
- The modular approach provides a balance between issue orientation and policy management.
- The policies created with this approach comprise individual modules, each created and updated by individuals responsible for the issues addressed.
- These individuals report to a central policy administration group that incorporates specific issues into an overall comprehensive policy.

Example ISSP Structure

- Statement of Policy
- Authorized Access and Usage of Equipment
- Prohibited Usage of Equipment
- Systems Management
- Violations of Policy
- Policy Review and Modification
- Limitations of Liability

Statement of Policy

- The policy should begin with a clear statement of purpose.
- Consider a policy that covers the issue of fair and responsible use of WWW and the Internet.
- The introductory section of this policy should outline these topics:
  - What is the scope of this policy?
  - Who is responsible and accountable for policy implementation?
  - What technologies and issues does it address?

Authorized Access and Usage of Equipment

- This section of the policy addresses who can use the technology governed by the policy, and what it can be used for.
- Remember that an organization's information systems are the exclusive property of the organization, and users have no particular right of use.
- Each technology and process is provided for business operations.
- Use for any other purpose constitutes misuse of equipment.
- This section defines "fair and responsible use" of equipment and other organizational assets, and should also address key legal issues such as protection of personal information and privacy.

Prohibited Usage of Equipment

- While the policy section details what the issue or technology can be used for, this section outlines what it cannot be used for.
- Unless a particular use is clearly prohibited, the organization cannot penalize its employees for misuse.
- The following can be prohibited: Personal Use, Disruptive use or misuse, criminal use, offensive or harassing materials, and infringement of copyrighted, licensed, or other intellectual property.

Systems Management

- There may be some overlap between an ISSP and a systems-specific policy, but the systems management section of the ISSP policy statement focuses on the user's relationship to systems management.
- Specific rules from management include regulating the use of e-mail, the storage of materials, authorized monitoring of employees, and the physical and electronic scrutiny of e-mail and other electronic documents.
- It is important that all such responsibilities are designated as belonging to either the systems administrator or the users; otherwise both parties may infer that the responsibility belongs to the other party.

Violations of Policy

- Once guidelines on equipment use have been outlined and responsibilities have been assigned, the individuals to whom the policy applies must understand the penalties and repercussions of violating the policy.
- Violations of policy should carry appropriate, not draconian, penalties.
- This section of the policy statement should contain not only the specifics of the penalties for each category of violation but also instructions on how individuals in the organization can report observed or suspected violations.
- Many individuals feel that powerful individuals in the organization can discriminate, single out, or other wise retaliate against someone who reports violations.
- Allowing anonymous submissions is often the only way to convince individual users to report the unauthorized activities of other, more influential employees.

Policy Review and Modification

- Because any document is only as good as its frequency of review, each policy should contain procedures and a timetable for periodic review.
- As the needs and technologies change in the organization, so must the policies that govern their use.
- This section should contain a specific methodology for the review and modification of the policy, to ensure that users do not begin circumventing it as it grows obsolete.

Limitations of Liability

- The final consideration is a general statement of liability or set of disclaimers
- If an individual employee is caught conducting illegal activities with organizational equipment or assets, management does not want the organization held liable.
- So the policy should state that if employees violate a company policy or any law using company technologies, the company will not protect them, and the company is not liable for its actions.
- It is inferred that such a violation would be without knowledge or authorization by the organization.

Systems-Specific Policy (SysSP)

While issue-specific policies are formalized as written documents, distributed to users, and agreed to in writing, SysSPs are frequently codified as standards and procedures to be used When configuring or maintaining systems

Systems-specific policies fall into two groups:

- Access control lists (ACLs) consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system.
  - An ACL is a list of access rights used by file storage systems, object brokers, or other network communications devices to determine which individuals or groups may access an object that it controls.(Object Brokers are system components that handle message requests between the software components of a system)

- A similar list, which is also associated with users and groups, is called a Capability Table. This specifies which subjects and objects a user or group can access. Capability tables are frequently complex matrices, rather than simple lists or tables.

- Configuration rules: comprise the specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.

ACL Policies

- ACL's allow configuration to restrict access from anyone and anywhere. Restrictions can be set for a particular user, computer, time, duration-even a particular file.

- ACL's regulate:
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system
  - Where authorized users can access the system from
  - How authorized users can access the system

- The WHO of ACL access may be determined by an individual person's identity or that person's membership in a group of people with the same access privileges.
- Determining WHAT users are permitted to access can include restrictions on the various attributes of the system resources, such as the type of resources (printers, files, communication devices, or applications), name of the resource, or the location of the resource.
- Access is controlled by adjusting the resource privileges for the person or group to one of Read, Write, Create, Modify, Delete, Compare, or Copy for the specific resource.
- To control WHEN access is allowed, some organizations choose to implement time-of-day and / or day-of-week restrictions for some network or system resources.
- For the control of WHERE resources can be accessed from, many network-connected assets have restrictions placed on them to block remote usage and also have some levels of access that are restricted to locally connected users.
- When these various ACL options are applied cumulatively, the organization has the ability to describe fully how its resources can be used.
- In some systems, these lists of ACL rules are known as Capability tables, user profiles, or user policies. They specify what the user can and cannot do on the resources within that system.

Rule Policies

- Rule policies are more specific to the operation of a system than ACL's
- Many security systems require specific configuration scripts telling the systems what actions to perform on each set of information they process
- Examples of these systems include firewalls, intrusion detection systems, and proxy servers.
- Fig 6.5 shows how network security policy has been implemented by Check Point in a firewall rule set.

VPN-1/Firewall-1 Policy Editor courtesy of Check Point Software Technologies Ltd.

FIGURE 6-5 Checkpoint VPN-1/Firewall-1 Policy Editor

Policy Management

- Policies are living documents that must be managed and nurtured, and are constantly changing and growing
- Documents must be properly disseminated (Distributed, read, understood, and agreed to) and managed
- Special considerations should be made for organizations undergoing mergers, takeovers, and partnerships
- In order to remain viable, policies must have:
  - an individual responsible for reviews
  - a schedule of reviews
  - a method for making recommendations for reviews
  - a specific effective and revision date

Responsible Individual

- The policy champion and manager is called the policy administrator.
- Policy administrator is a mid-level staff member and is responsible for the creation, revision, distribution, and storage of the policy.
- It is good practice to actively solicit input both from the technically adept information security experts and from the business-focused managers in each community of interest when making revisions to security policies.
- This individual should also notify all affected members of the organization when the policy is modified.
- The policy administrator must be clearly identified on the policy document as the primary point of contact for additional information or for revision suggestions to the policy.

Schedule of Reviews

- Policies are effective only if they are periodically reviewed for currency and accuracy and modified to reflect these changes.
- Policies that are not kept current can become liabilities for the organization, as outdated rules are enforced or not, and new requirements are ignored.
- Organization must demonstrate with due diligence, that it is actively trying to meet the requirements of the market in which it operates.
- A properly organized schedule of reviews should be defined (at least annually) and published as part of the document.

Review Procedures and Practices

- To facilitate policy reviews, the policy manager should implement a mechanism by which individuals can comfortably make recommendations for revisions.
- Recommendation methods can involve e-mail, office mail, and an anonymous drop box.
- Once the policy Hs come up for review, all comments should be examined and management –approved improvements should be implemented.

- Most policies are drafted by a single, responsible individual and are then reviewed by a higher-level manager.
- But even this method should not preclude the collection and review of employee input.

Policy and Revision Date

- When policies are drafted and published without a date, confusion can arise when users of the policy's age or status.
- If policies are not reviewed and kept current, or if members of the organization are following undated versions, disastrous results and legal headaches can ensue.
- It is therefore, important that the policy contain the date of origin, along with the date(s) of any revisions.
- Some policies may also need a SUNSET clause indicating their expiration date.
- Automation can streamline the repetitive steps of writing policy, tracking the workflow of policy approvals, publishing policy once it is written and approved, and tracking when individuals have read the policy.
- Using techniques from computer based training and testing, organizations can train staff members and also improve the organization's awareness program.
- NetIQ corporation quotes that:
  - SOFTWARE THAT PUTS YOU IN CONTROL OF SECURITY POLICY CREATION, DISTRIBUTION, EDUCATION, AND TRACKING FOR COMPLIANCE
  - VigilEnt Policy Center makes it possible to manage security policy dynamically so that you can create, distribute, educate, and track understanding of information security policies for all employees in the organization.
  - It enables to keep policies up-to-date, change them quickly as needed, and ensure that they are being understood properly, all through a new automated, interactive, web-based software application.

Information and Network Security Notes eBook

Publisher : VTU eLearning

Author :

Type the URL : http://www.kopykitab.com/product/1836

Get this eBook