

# 3

## Security Policies, Standards, and Planning

You got to be careful if you don't know where you're going, because you might not get there.

**YOGI BERRA**

**MATTHIAS WAS READY TO APPLY THE FIREWALL** scripts to protect the servers belonging to ATI's clients. The *Linen Planet* had hired ATI to design, configure, and operate the network and defenses used to implement the electronic commerce startup's business plan. Matthias had a text file with more than 300 scripted instructions that had to be added to the firewall.

Since this change would affect the client's entire network, it was being tested in tonight's third-shift change-window, a time-slot during which network technicians could interrupt the normal operation of the network for a short time. Even though Matthias had only recently become involved in this project, it had been under development for several weeks, and the activities planned for tonight had been approved by the change control committees at *Linen Planet* and at ATI.

The plan was for Matthias to update the firewall command interface and be ready to commit the new rules at 2:30 AM. He had already made the connection and edited the file, and he was waiting to commit the new rules so the quality assurance testing team could spend an hour furiously testing the new configuration. At the first sign of a test failure, they would tell Matthias to back out the changes and reset the firewall to its original configuration.

He had a few minutes to wait, and Al sat down next to him to monitor the event.

Matthias said, "Hi Al. I have a question."

Al looked over his arm at the monitor to review Matthias's work. Seeing it was all in order and that the commit time was still a few minutes away, he said, "OK. Shoot."

Matthias pointed at the work order with the attached script of complex firewall rules and said, "Who writes these rules, and how do they know what the rules should do?"

Al looked at him and said, "One word—policy."

"Huh," said Matthias. "What does that mean?"

"Well," said Al, "Every company has a set of policies that let everyone know what they can and can't do with the company network. *Linen Planet* has an enterprise policy and a network usage policy that specify how they manage their network. Also, they have certain technical control systems in place, like intrusion detection systems that need to operate on their network. Our engineers take all of these factors into account and write rules that they hope will make it all work."

"Oh," said Matthias. "Well, it's time to commit these rules."

He pressed the Enter button on his keyboard.

## LEARNING OBJECTIVES:

Upon completion of this material, you should be able to do the following:

- Define management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
- Describe an information security blueprint, identify its major components, and explain how it is used to support a network security program
- Discuss how an organization institutionalizes policies, standards, and practices using education, training, and awareness programs
- Explain contingency planning, and describe the relationships among incident response planning, disaster recovery planning, business continuity planning, and contingency planning

## Introduction

In order to most effectively secure its network environment, an organization must establish a functional and well-designed information security program. Firewalls, network security, and intrusion detection systems can only succeed within the context of a well-planned and fully defined information security program. Uncoordinated security initiatives are seldom as effective as those that operate under a complete and effective policy environment. The creation of an information security program begins with the creation or review of the organization's information security policies, standards, and practices, followed by the selection or creation of information security architecture and a detailed information security blueprint. Without policy, blueprints, and planning, the organization will not be able to meet the information security needs of the various communities of interest. The role of planning in the modern organization is hard to overemphasize. All but the smallest organizations 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 must make policies the basis for all information security planning, design, and deployment. Policies direct how issues are addressed and how technologies are used. Policies do not specify the proper operation of equipment or software—this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation. In addition, *policy should never contradict law*, because this can create a significant liability for the organization.

Because information security is primarily a management problem, not a technical one, quality security programs begin and end with policy.<sup>1</sup> Policy obliges personnel to function in a manner that adds to the security of information assets, rather than threatening them. Security policies are the least expensive control to design and disseminate—they require only the time and effort of the management team—but the most difficult to implement *properly*. Even if the management team hires an outside consultant to assist in the development of policy, the costs are minimal compared to those of technical controls. However, shaping policy is difficult because policy must:

- Never conflict with laws
- Stand up in court, if challenged
- Be properly administered through dissemination and documented acceptance

For a policy to be considered effective and legally enforceable, it must meet the following criteria:

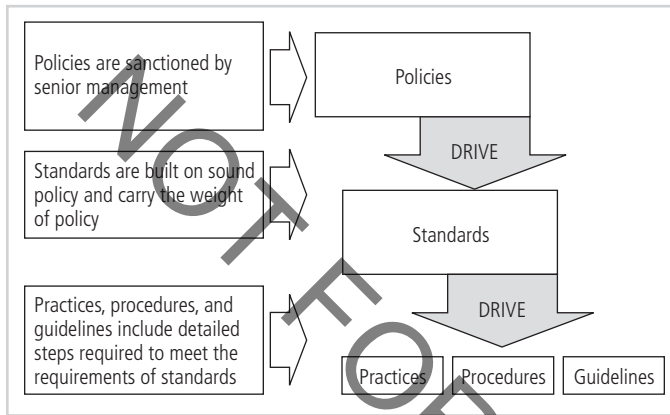
- Dissemination (distribution)—The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard-copy and electronic distribution.
- Review (reading)—The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Often organizations record versions of the policy in English and alternate languages.
- Comprehension (understanding)—The organization must be able to demonstrate that employees understood the requirements and content of the policy. Common techniques include quizzes and other assessments.
- Compliance (agreement)—The organization must be able to demonstrate that employees agree to comply with the policy, through act or affirmation. Common techniques include logon banners that require a specific action (mouse click or keystroke) to acknowledge agreement, or requiring employees to sign a document clearly indicating that they have read, understood, and agreed to comply with the policy.
- Uniform enforcement—The organization must be able to demonstrate that the policy has been uniformly enforced.

### Definitions

Before examining the various types of information security policies, it is important to understand exactly what policy is and how it can and should be used.

A **policy** is a set of guidelines or instructions that an organization's senior management implements to regulate the activities of the members of the organization who make

decisions, take actions, and perform other duties. Policies are organizational laws in that they dictate acceptable and unacceptable behavior within the organization. Like laws, policies define what is right and what is wrong, what the penalties are for violating policy, and what the appeal process is. **Standards**, though they have the same compliance requirement as policies, are more detailed descriptions of what must be done to comply with policy. The standards may be informal, or part of an organizational culture, as in **de facto standards**. Or standards may be published, scrutinized, and ratified by a group, as formal or **de jure standards**. Practices, procedures, and guidelines effectively explain how to comply with policy. Figure 3-1 shows policies as the force that drives standards, which in turn drive practices, procedures, and guidelines.



**FIGURE 3-1** Policies, Standards, and Practices

Policies are put in place to support the organization's mission, vision, and strategic planning. The **mission** of an organization is a written statement of an organization's purpose. The **vision** of an organization is a written statement of the organization's long-term goals—where will the organization be in five years? In ten? **Strategic planning** is the process of moving the organization towards its vision.

The meaning of the term **security policy** depends on the context in which it is used. Governmental agencies discuss security policy in terms of national security and national policies to deal with foreign states. A security policy can also be a credit card agency's method of 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.

Management must define three types of security policies, according to The National Institute of Standards and Technology's Special Publication 800-14:

1. Enterprise information security policies
2. Issue-specific security policies
3. System-specific security policies

Each of these management policies is examined in greater detail in the sections that follow.

## Enterprise Information Security Policy (EISP)

An **enterprise information security policy (EISP)** is also known as a general security policy, IT security policy, or information security policy. 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. The EISP is an executive-level document, usually drafted by, or in cooperation with, the chief information officer of the organization. This policy is usually two to ten pages long and shapes the philosophy of security in the IT environment. The EISP usually needs to be modified only when there is a change in the strategic direction of the organization.

The EISP guides the development, implementation, and management of the security program. It specifies the requirements to be met by the information security blueprint or framework. It defines the 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 the National Institute of Standards and Technology, the EISP typically addresses compliance in two areas:

- (1) General compliance to ensure meeting the requirements to establish a program and the responsibilities assigned therein to various organizational components and
- (2) the use of specified penalties and disciplinary action.<sup>2</sup>

When the EISP has been developed, the CISO (chief information security officer) begins forming the security team and initiating the necessary changes to the information security program.

### EISP Elements

Although the specifics of EISPs vary from organization to organization, most EISP documents should include the following elements:

- An overview of the corporate philosophy on security
- Information on the structure of the information security organization and individuals who fulfill the information security role
- Fully articulated security responsibilities that are shared by all members of the organization (employees, contractors, consultants, partners, and visitors)
- Fully articulated security responsibilities that are unique to each role within the organization

The components of a good EISP are shown in Table 3-1.<sup>3</sup>

**TABLE 3-1** Components of the EISP

Component	Description
Statement of Purpose	<p>Answers the question, “What is this policy for?” Provides a framework that helps the reader to understand the intent of the document. For example:</p> <p>“This document will:</p> <ul style="list-style-type: none"> <li>Identify the elements of a good security policy</li> <li>Explain the need for information security</li> <li>Specify the various categories of information security</li> <li>Identify the information security responsibilities and roles</li> <li>Identify appropriate levels of security through standards and guidelines</li> </ul> <p>This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.”<sup>4</sup></p>
Information Technology Security Elements	<p>Defines information security. For example:</p> <p>“Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology...”</p> <p>This section can also lay out security definitions or philosophies to clarify the policy.</p>
Need for Information Technology Security	<p>Provides information on the importance of information security in the organization and the obligation (legal and ethical) to protect critical information about customers, employees, and markets.</p>
Information Technology Security Responsibilities and Roles	<p>Defines the organizational structure designed to support information security. Identifies categories of individuals with responsibility for information security (IT department, management, users) and their information security responsibilities, including maintenance of this document.</p>
Reference to Other Information Technology Standards and Guidelines	<p>Lists other standards that influence and are influenced by this policy document, perhaps including relevant laws (federal and state) and other policies.</p>

### Issue-Specific Security Policy (ISSP)

As an organization executes various technologies and processes to support routine operations, it must instruct employees on the proper use of those technologies and processes. In general, the **issue-specific security policy**, or **ISSP**, (1) addresses specific areas of technology as listed below, (2) requires frequent updates, and (3) contains a statement on the

organization's position on a specific issue.<sup>5</sup> An ISSP may cover the following topics, among others:

- Use of company-owned networks and the Internet
- Use of telecommunications technologies (fax and phone)
- Use of electronic mail
- 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 photocopy equipment

There are a number of approaches to creating and managing ISSPs within an organization. Three of the most common are to create the following types of ISSP documents:

1. Independent ISSP documents, each tailored to a specific issue
2. A single comprehensive ISSP document covering all issues
3. A modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements

The independent ISSP document 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 may fail to cover all of the necessary issues, and can lead to poor policy distribution, management, and enforcement.

The single comprehensive ISSP is centrally managed and controlled. With formal procedures for the management of ISSPs in place, the comprehensive policy approach establishes guidelines for issue coverage and clearly identifies processes for the dissemination, enforcement, and review of these guidelines. Usually, comprehensive ISSPs are developed by those responsible for managing the information technology resources. Unfortunately, they tend to overly generalize the issues and skip over vulnerabilities.

The optimal balance between the independent and comprehensive ISSP is the modular ISSP. It is also centrally 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 via 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.

Table 3-2 shows an outline of a sample ISSP, which can be used as a model. An organization should add to this structure any security procedures not covered by these general guidelines.

**TABLE 3-2** Components of an Effective Use Policy

- |                                                               |
|---------------------------------------------------------------|
| 1. Statement of policy                                        |
| a. Scope and applicability                                    |
| b. Definition of technology addressed                         |
| c. Responsibilities                                           |
| 2. Authorized access and usage                                |
| a. User access                                                |
| b. Fair and responsible use                                   |
| c. Protection of privacy                                      |
| 3. Prohibited usage                                           |
| a. Disruptive use or misuse                                   |
| b. Criminal use                                               |
| c. Offensive or harassing materials                           |
| d. Copyrighted, licensed, or other intellectual property      |
| e. Other restrictions                                         |
| 4. Systems management                                         |
| a. Management of stored materials                             |
| b. Employee monitoring                                        |
| c. Virus protection                                           |
| d. Physical security                                          |
| e. Encryption                                                 |
| 5. Violations of policy                                       |
| a. Procedures for reporting violations                        |
| b. Penalties for violations                                   |
| 6. Policy review and modification                             |
| a. Scheduled review of policy and procedures for modification |
| 7. Limitations of liability                                   |
| a. Statements of liability or disclaimers                     |

The components of each of the major categories presented in the sample issue-specific policy shown in Table 3-2 are discussed below. Even though the details may vary from policy to policy and some sections of a modular policy may be combined, it is essential for management to address and complete each section.

### 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 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

This section of the policy statement 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 general rights of use. Each technology and process is provided for business operations. Use for any other purpose constitutes misuse. This section defines "fair and responsible use" of the covered

technology and other organizational assets, and should also address key legal issues, such as protection of personal information and privacy.

### **Prohibited Use**

Unless a particular use of technology is clearly prohibited, the organization cannot penalize its employees for using it in that fashion. 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. An alternative approach collapses categories 2 and 3 of Table 3-2 into a single category—appropriate use. Many organizations use an ISSP titled “Appropriate Use” to cover both categories.

### **Systems Management**

The systems management section of the ISSP policy statement focuses on users’ relationships to systems management. Specific management rules 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 be designated to either the systems administrators or the users; otherwise, both parties may infer that the responsibility belongs to the other party.

### **Violations of Policy**

Once guidelines on use have been outlined and responsibilities have been assigned, the policy must specify the penalties for, and repercussions of, policy violation. Violations should incur appropriate, not draconian, penalties. This section of the policy statement should specify the penalties for each category of violation as well as instructions on how individuals in the organization can report observed or suspected violations. Many people think that powerful individuals in the organization can discriminate, single out, or otherwise retaliate against someone who reports violations. Allowing anonymous submissions is often the only way to convince users to report the unauthorized activities of other, more influential employees.

### **Policy Review and Modification**

Because a document is only useful if it is up to date, each policy should contain procedures and a timetable for periodic review. As the organization’s needs and technologies change, so must the policies that govern their use. This section should specify a 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**

If an employee is caught conducting illegal activities with organizational equipment or assets, management does not want the organization held liable. The policy should state that the organization will not protect employees who violate a company policy or any law using company technologies, and that the company is not liable for such actions. It is understood that such violations are without the organization’s knowledge or authorization.

### **System-Specific Policy (SysSP)**

While issue-specific policies are written documents readily identifiable as policy, system-specific security policies (SysSPs) sometimes have a different look. SysSPs often function as standards or procedures to be used when configuring or maintaining systems. For example, a

SysSP might describe the configuration and operation of a network firewall. This document could include a statement of managerial intent; guidance to network engineers on the selection, configuration, and operation of firewalls; and an access control list that defines levels of access for each authorized user. SysSPs can be separated into two general groups, **managerial guidance** and **technical specifications**, or they can be combined into a single policy document.

### Managerial Guidance SysSPs

A managerial guidance SysSP document is created by management to guide the implementation and configuration of technology as well as to regulate the behavior of people in the organization. For example, while the method for implementing a firewall belongs in the technical specifications SysSP, the firewall's configuration must follow guidelines established by management. An organization might not want its employees to have access to the Internet via the organization's network, for instance; in that case, the firewall would have to be implemented accordingly.

Firewalls are not the only technology that may require system-specific policies. Any system that affects the confidentiality, integrity, or availability of information must be assessed to evaluate the trade-off between improved security and restrictions.

System-specific policies can be developed at the same time as ISSPs, or they can be prepared in advance of their related ISSPs. Before management can craft a policy informing users what they can do with the technology and how they can accomplish this, it might be necessary for system administrators to configure and operate the system. Some organizations may prefer to develop ISSPs and SysSPs in tandem, so that operational procedures and user guidelines are created simultaneously.

### Technical Specifications SysSPs

While a manager can work with a systems administrator to create managerial policy, the system administrator may in turn need to create a policy to implement the managerial policy. Each type of equipment requires its own set of policies to translate the managerial intent into an enforceable technical approach. For example, an ISSP may require that user passwords be changed quarterly; a systems administrator can implement a technical control within a specific application to enforce this policy. There are two general methods of implementing such technical controls: access control lists and configuration rules.

**Access control lists** (ACLs) consist of the user access lists, matrices, and capability tables that govern the rights and privileges of users. ACLs can control access to file storage systems, software components, or network communications devices. A **capability table** specifies which subjects and objects users or groups can access; in some systems, capability tables are called user profiles or user policies. These specifications frequently take the form of complex matrices, rather than simple lists or tables. The **access control matrix** includes a combination of tables and lists, such that organizational assets are listed along the column headers, while users are listed along the row headers. The resulting matrix contains ACLs in columns for a particular device or asset, while a row contains the capability table for a particular user.

Operating systems translate ACLs into sets of configurations that administrators use to control access to their systems. The level of detail may differ from system to system, but in general ACLs can restrict access for a particular user, computer, time, duration—even a particular file. This specificity provides powerful control to the administrator. In general ACLs 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

The *who* of ACL access may be determined by a person's identity or by a person's membership in a group. Restricting *what* authorized users are permitted to access—whether by resource type (printers, files, communication devices, or applications), name, or location—is achieved by adjusting the resource privileges for a person or group to Read, Write, Create, Modify, Delete, Compare, or Copy. To control *when* access is allowed, some organizations implement time-of-day and/or day-of-week restrictions for some network or system resources. To control *where* resources can be accessed from, many network-connected assets block remote usage and also have some levels of access that are restricted to locally connected users. When these various ACL options are applied concurrently, the organization has the ability to govern how its resources can be used. The implementation of ACLs to manage firewalls is fully explored in other chapters of this book.

**Configuration rule policies** are the specific instructions entered into a security system, to regulate how it reacts to the data it receives. Rule-based policies are more specific to the operation of a system than ACLs are, and they may or may not deal with users directly. Many security systems, for example firewalls, intrusion detection systems (IDSs), and proxy servers, use specific configuration scripts that represent the configuration rule policy, to determine how the system handles each data element it processes.

### Combination SysSPs

Many organizations create a single document that combines the management guidance SysSP and the technical specifications SysSP. While this document can be somewhat confusing to casual users, it is practical to have the guidance from both managerial and technical perspectives in a single place. If this approach is employed, care should be taken to clearly articulate the required actions. Some might consider this type of policy document a procedure, but it is actually a hybrid that combines policy with procedural guidance for the convenience of the implementers of the system being managed. This approach is successfully used by organizations that have multiple technical control systems of different types, and by smaller organizations that are seeking to document policy and procedure in a compact format.

## Policy Management

Policies are living documents that must be managed and nurtured. It is unacceptable to create such an important set of documents and then shelve them. These documents must be properly disseminated (distributed, read, understood, and agreed to) and managed. How they are managed relates directly to the policy management section of the issue-specific policy described earlier. Good management practices for policy development and maintenance make for a more resilient organization. For example, all policies, including security policies, undergo tremendous stress when corporate mergers and divestitures occur; in such situations employees are faced with uncertainty and many distractions. System vulnerabilities can arise if, for instance, incongruous security policies are implemented in different parts of a new, merged organization. When two companies merge but retain separate policies, the difficulty of implementing security controls increases. Likewise, when one company with unified policies splits in two, each new company may require different policies.

To remain viable, security policies must have one or more responsible individuals assigned to manage them, a schedule of reviews, a method for making recommendations for reviews, and a policy issuance and revision date. Each of these is examined in additional detail below.

### Responsible Individual

Just as information systems and information security projects must have champions and managers, so must policies. The policy champion and manager is called the **policy administrator**. Typically the policy administrator is a mid-level staff member and is responsible for the creation, revision, distribution, and storage of the policy. Note that the policy administrator position does not necessarily require technical expertise. While practicing information security professionals require extensive technical knowledge; policy management and policy administration require only a moderate technical background. It is good practice, however, for policy administrators to 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. The administrator should also notify all affected members of the organization when the policy is modified.

It is disheartening when a policy that required hundreds of staff-hours to develop and document is ignored. Thus, someone must be responsible for placing the policy and all subsequent revisions into the hands of those who are accountable for its implementation. 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 can only retain their effectiveness in a changing environment if they are periodically reviewed for currency and accuracy and modified accordingly. Out-of-date policies can become liabilities, as outdated rules are enforced (or not), and new requirements are ignored. In order to demonstrate due diligence, an organization must demonstrate that it is actively trying to meet the requirements of the market in which it operates. This applies to both public (government, academic, and nonprofit) and private (commercial and for-profit) organizations. A properly organized schedule of reviews should be defined and published as part of the document. Typically a policy should be reviewed at least annually to ensure that it is still an effective control.

### Review Procedures and Practices

To facilitate policy reviews, the policy manager should implement a mechanism to enable people to make recommendations for revisions. Recommendation methods can involve e-mail, office mail, and an anonymous drop box. If the policy is controversial, the policy administrator may feel that anonymous submission of information is the best way to solicit staff opinions. Many employees are intimidated by management and hesitate to voice honest opinions about a policy unless they can do so anonymously. Once the policy has come up for review, all comments should be examined, and management-approved improvements should be implemented. Additional review methods can include representative users in the revision process and solicit direct comment on the revision of the policy. In reality, most policies are drafted by a single, responsible individual and 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

The simple act of dating the policy is often skipped. When policies are published without dates, confusion can arise. 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. These problems are particularly common in high-turnover environments. 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**, which provides an expiration date—particularly in policies that govern information use in short-term business associations or in agencies that become involved with the organization. Establishing a policy end date prevents a temporary policy from mistakenly becoming permanent, and it also enables an organization to gain experience with a given policy before adopting it permanently.

### Automated Policy Management

Recent years have seen the emergence of a new category of software for managing information security policies. This type of software was developed in response to needs articulated by information security practitioners. While there have been many software products that meet the need for a specific technical control, there is now software that meets the need for automating some of the busywork of policy management. Automation can streamline the process of writing policy, tracking the workflow of policy approvals, publishing policy once it is written and approved, and tracking policy distribution and compliance agreement. Using techniques from computer-based training and testing, organizations can train staff members and also improve the organization's awareness program. Once an organization has developed its information security policies and standards, the information security community can begin developing the blueprint for the information security program. If one or more components of policies, standards, or practices are incomplete, management must determine whether or not to nonetheless proceed with the development of the blueprint.

---

## Frameworks and Industry Standards

After the information security team has inventoried the organization's information assets and assessed and prioritized the threats to those assets, it must conduct a series of risk assessments using quantitative or qualitative analyses, as well as feasibility studies and cost-benefit analyses. These assessments, which include determining each asset's current protection level, are used to decide whether or not to proceed with any given control. Armed with a general idea of the vulnerabilities in the information technology systems, the security team develops a design blueprint for security, which is used to implement the security program.

This **security blueprint** is the basis for the design, selection, and implementation of all security program elements, including policy implementation, ongoing policy management, risk management programs, education and training programs, technological controls, and maintenance of the security program. The security blueprint, built on top of the organization's information security policies, is a scalable, upgradable, comprehensive plan to meet the organization's current and future information security needs. It is a detailed version of the **security framework**, which is an outline of the overall information security strategy and a roadmap for planned changes to the organization's information security environment. The blueprint specifies the tasks in the order in which they are to be accomplished.

To select a methodology by which to develop an information security blueprint, you can adapt or adopt a published information security model or framework. This framework can be an outline of steps to take to design and implement information security in the organization. There are a number of published information security frameworks, including ones from government sources, which are presented later in this chapter. Because each information security environment is unique, the security team may need to modify or adapt pieces from several frameworks; what works well for one organization may not precisely fit another.

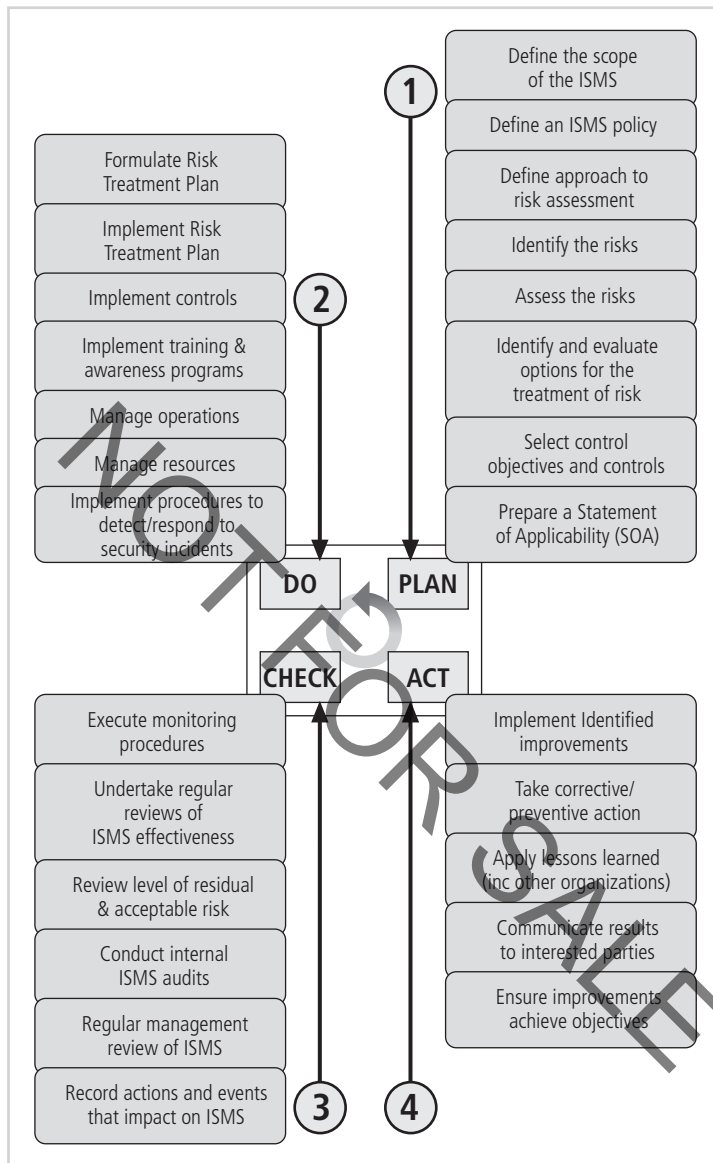
## The ISO 27000 Series

One of the most widely referenced security models is the *Information Technology—Code of Practice for Information Security Management*, which was originally published as British Standard BS7799. In 2000, this Code of Practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799. The document was revised in 2005 (becoming ISO 17799:2005), and it was renamed ISO 27002 in 2007, to align it with the document ISO 27001, discussed later in this chapter. While the details of ISO/IEC 27002 are available to those who purchase the standard, its structure and general organization are well known. For a summary description, see Table 3-3. For more details on ISO/IEC Sections, see [www.praxiom.com/iso-17799-2005.htm](http://www.praxiom.com/iso-17799-2005.htm).

**TABLE 3-3** The Sections of the ISO/IEC 27002<sup>6</sup>

1. Risk Assessment and Treatment
2. Security Policy
3. Organization of Information Security
4. Asset Management
5. Human Resource Security
6. Physical and Environmental Security
7. Communications and Operations
8. Access Control
9. Information Systems Acquisition, Development and Maintenance
10. Information Security Incident Management
11. Business Continuity Management
12. Compliance

The stated purpose of ISO/IEC 27002 is to “give recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings.”<sup>7</sup> Where ISO/IEC 27002 offers a broad overview of the various areas of security, providing information on 127 controls over ten broad areas, ISO/IEC 27001 provides information on how to implement ISO/IEC 27002 and how to set up an information security management system (ISMS). The overall methodology for this process and its major steps are presented in Figure 3-2.



Courtesy of Gamma Secure Systems

**FIGURE 3-2** BS7799:2 Major Process Steps<sup>8</sup>

In the United Kingdom, correct implementation of these standards (both volumes), as determined by a BS7799 certified evaluator, allows organizations to obtain system (ISMS) certification and accreditation. When the standard first came out, several countries including the United States, Germany, and Japan refused to adopt it, on the grounds that there are several fundamental problems, including:

- The global information security community has not defined any justification for a code of practice as was identified in the ISO/IEC 17799.

- ISO/IEC 17799 lacked “the necessary measurement precision of a technical standard.”<sup>9</sup>
- There is no reason to believe that ISO/IEC 17799 was more useful than any other approach.
- ISO/IEC 17799 was not as complete as other frameworks.
- ISO/IEC 17799 was hurriedly prepared given the tremendous impact its adoption could have on industry information security controls.<sup>10</sup>

ISO/IEC 27002 is an interesting framework for information security, but aside from those relatively few U.S. organizations that operate in the European Union (or are otherwise obliged to meet its terms), most U.S. organizations are not expected to comply with this standard.

### **ISO/IEC 27001:2005: The Information Security Management System**

ISO/IEC 27001 provides implementation details using a Plan-Do-Check-Act cycle, as described in Table 3-4 and shown in Figure 3-3 in abbreviated form:

**TABLE 3-4** The ISO/IEC 27001:2005 Plan-Do-Check-Act Cycle

**Plan:**

1. Define the scope of the ISMS.
2. Define an ISMS policy.
3. Define the approach to risk assessment.
4. Identify the risks.
5. Assess the risks.
6. Identify and evaluate options for the treatment of risk.
7. Select control objectives and controls.
8. Prepare a Statement of Applicability (SOA).

**Do:**

9. Formulate a Risk Treatment Plan.
10. Implement the Risk Treatment Plan.
11. Implement controls.
12. Implement training and awareness programs.
13. Manage operations.
14. Manage resources.
15. Implement procedures to detect and respond to security incidents.

**TABLE 3-4** The ISO/IEC 27001:2005 Plan-Do-Check-Act Cycle (continued)**Check:**

- 
16. Execute monitoring procedures.

---

  17. Undertake regular reviews of ISMS effectiveness.

---

  18. Review the level of residual and acceptable risk.

---

  19. Conduct internal ISMS audits.

---

  20. Undertake regular management review of the ISMS.

---

  21. Record actions and events that impact an ISMS.

---

**Act:**

- 
22. Implement identified improvements.

---

  23. Take corrective or preventive action.

---

  24. Apply lessons learned.

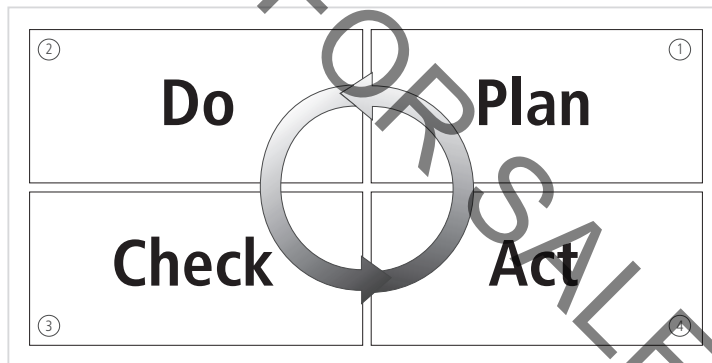
---

  25. Communicate results to interested parties.

---

  26. Ensure improvements achieve objectives.<sup>11</sup>

---

**FIGURE 3-3** BS7799:2 —Plan-Do-Check-Act

Although ISO/IEC 27001 provides some implementation information, it simply specifies *what* must be done—not *how* to do it. As noted by Gamma Secure Systems, “The standard has an appendix that gives guidance on the use of the standard, in particular to expand on the Plan-Do-Check-Act concept. It is important to realize that there will be many Plan-Do-Check-Act cycles within a single ISMS all operating asynchronously at different speeds.”<sup>12</sup>

As stated earlier, ISO/IEC 27001’s primary purpose is to enable organizations that adopt it to obtain certification, and thus serves better as an assessment tool than an implementation framework.

In 2007, the International Organization for Standardization announced the plans for the numbering of current and forthcoming standards related to information security issues and topics, as shown in table 3-5.

**TABLE 3-5** ISO 27000 Series Current and Planned Standards

ISO 27000 Series Standard	Status	Title or Topic	Comment
27000	Planned	Series Overview and Terminology	Typically when ISO releases a series of standards, the first defines series terminology and vocabulary.
27001	2005	Information Security Management System Specification	Drawn from BS 7799:2.
27002	2007	Code of Practice for Information Security Management	Was renamed from ISO/IEC 17799, drawn from BS 7799:1.
27003	Planned	Information Security Management Systems Implementation Guidelines	Expected 2008.
27004	Planned	Information Security Measurements and Metrics	Expected 2008.
27005	Planned	ISMS Risk Management	Expected in 2008 or later.
27006	2007	Requirements for Bodies Providing Audit and Certification of an ISMS	Is largely intended to support the accreditation of certification bodies providing ISMS certification.

## NIST Security Models

Another possible approach is described in documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (*csrc.nist.gov*). Because the NIST documents are publicly available, free, and have been available for some time, they have been broadly reviewed by government and industry professionals, and were among the references cited by the federal government when it decided not to select the ISO/IEC 17799 standards. The following NIST documents can assist in the design of a security framework:

- SP 800-12: *An Introduction to Computer Security: The NIST Handbook*
- SP 800-14: *Generally Accepted Principles and Practices for Securing Information Technology Systems*
- SP 800-18 Rev. 1: *Guide for Developing Security Plans for Federal Information Systems*
- SP 800-26: *Security Self-Assessment Guide for Information Technology Systems*
- SP 800-30: *Risk Management Guide for Information Technology Systems*

### NIST Special Publication SP 800-12

SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, 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 design and implementation of new security systems, and therefore should be used only as a precursor to understanding an information security blueprint.

### **NIST Special Publication 800-14**

*Generally Accepted Principles and Practices for Securing Information Technology Systems* provides best practices and security principles that can direct the security team in the development of a security blueprint. In addition to detailing security best practices across the spectrum of security areas, it provides philosophical principles that the security team should integrate into the entire information security process. The document can guide the development of the security framework and should be combined with other NIST publications providing the necessary structure to the entire security process.

### **NIST Special Publication 800-18 Rev. 1**

The *Guide for Developing Security Plans for Federal Information Systems* can be used as the foundation for a comprehensive security blueprint and framework. This publication provides detailed methods for assessing, designing, and implementing controls and plans for applications of varying size. SP 800-18 Rev. 1 can serve as a useful guide to the information security planning process. It also includes templates for major application security plans. As with any publication of this scope and magnitude, SP 800-18 Rev. 1 must be customized to fit the particular needs of an organization.

### **IETF Security Architecture**

The Security Area Working Group acts as an advisory board for the protocols and areas developed and promoted by the Internet Society and the Internet Engineering Task Force (IETF), and while the group endorses no specific information security architecture, one of its requests for comment (RFC), RFC 2196: *Site Security Handbook*, offers a good discussion of important security issues. RFC 2196: *Site Security Handbook* covers five basic areas of security with detailed discussions on development and implementation. There are also chapters on such important topics as security policies, security technical architecture, security services, and security incident handling.

### **Benchmarking and Best Business Practices**

Benchmarking and best practices are reliable methods used by some organizations to assess security practices. Benchmarking and best practices don't provide a complete methodology for the design and implementation of all the practices needed by an organization; however, it is possible to put together the desired outcome of the security process, and to work backwards toward an effective design. The Federal Agency Security Practices (FASP) site, [fasp.nist.gov](http://fasp.nist.gov), is a popular place to look up best practices. FASP is designed to provide best practices for public agencies, but these practices can be adapted easily to private institutions. The documents found in this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel. Of particular value is the section on program management, which includes:

- A summary guide: public law, executive orders, and policy documents
- Position description for computer system security officer
- Position description for information security officer
- Position description for computer specialist

- Sample of an information technology (IT) security staffing plan for a large service application (LSA)
- Sample of information technology (IT) security program policy
- Security handbook and standard operating procedures
- Telecommuting and mobile computer security policy

In the later stages of information security blueprint creation, these policy documents are particularly useful.

A number of other public and semipublic institutions provide information on best practices. One of these groups is the EDUCAUSE Computer and Network Security Task Force ([http://www.educause.edu/content.asp?SECTION\\_ID=30](http://www.educause.edu/content.asp?SECTION_ID=30)), which is a non-profit group that provides resources for higher education. This group focuses on the impact of Internet security in higher education, but provides valuable resources for any organization that uses the Internet, including many recommendations for security implementations. Another widely referenced source is the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University ([www.cert.org](http://www.cert.org)). CERT/CC provides detailed and specific assistance on how to implement a sound security methodology.

Professional societies often provide information on best practices to their members. The Technology Managers Forum ([www.techforum.com](http://www.techforum.com)) has an annual best practice award in a number of areas, including information security. The Information Security Forum ([www.isfsecuritystandard.com](http://www.isfsecuritystandard.com)) has a free publication titled “Standard of Good Practice.” This publication outlines information security best practices.

Many organizations hold seminars and classes on best practices for implementing security; in particular the ISACA ([www.isaca.org](http://www.isaca.org)) hosts regular seminars. The International Association of Professional Security Consultants ([www.iapsc.org](http://www.iapsc.org)) has a listing of best practices, as does the Open Grid Forum ([www.ogf.org](http://www.ogf.org)). At a minimum, information security professionals can peruse Web portals for posted security best practices. There are several free portals dedicated to security that have collections of best practices, such as SearchSecurity.com, and NIST’s Computer Resources Center. These are but a few of the many public and private organizations that promote solid best security practices. Investing a few hours searching the Web reveals dozens of locations for additional information.

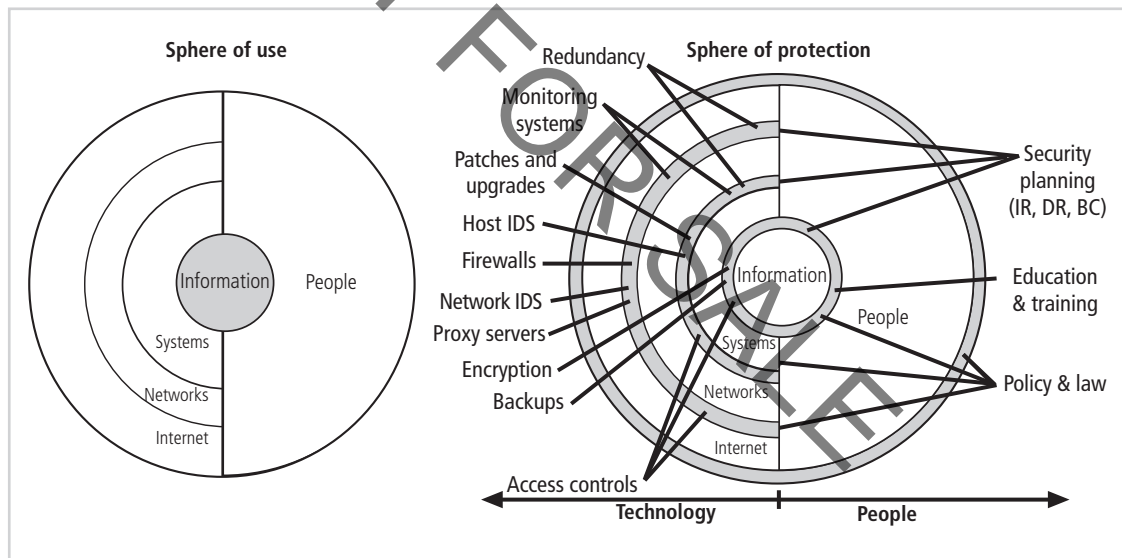
## Security Architecture

To further the discussion of information security program architecture and to illustrate industry best practices, the following sections outline a few key security architectural components. Many of these components are examined in detail in later chapters, but an overview is provided here.

### Spheres of Security

The spheres of security, shown in Figure 3-4, are the foundation of the security framework. Generally speaking, the spheres of security illustrate how information is under attack from a variety of sources. The sphere of use, on the left-hand side of Figure 3-4, illustrates the ways in which people access information; for example, people read hard copies of documents, and can also access information through systems. Information, as the most important asset in this model, is at the center of the sphere. Information is always at risk from the people and computer systems that have access to it. Networks and

the Internet represent indirect threats, because a person attempting to access information from the Internet must first go through the local networks and then access systems that contain the information. The sphere of protection, on the right-hand side of Figure 3-4, illustrates that between each layer of the sphere of use there must exist a layer of protection to prevent access to the inner layer from the outer layer. Each shaded band is a layer of protection and control. For example, the items labeled “Policy & law” and “Education & training” are located between people and the information. Controls are also implemented between systems and the information, between networks and the computer systems, and between the Internet and internal networks. This reinforces the concept of defense in depth. As illustrated in the sphere of protection, a variety of controls can be used to protect the information. The items of control shown in the figure are not intended to be comprehensive, but illustrate individual safeguards that can protect the various systems that are located closer to the center of the sphere. However, because people can directly access each ring as well as the information at the core of the model, the side of the sphere of protection that attempts to control access by relying on people requires a different approach to security than the side that uses technology. The members of the organization must become a safeguard that is effectively trained, implemented, and maintained, or they too represent a threat to the information.

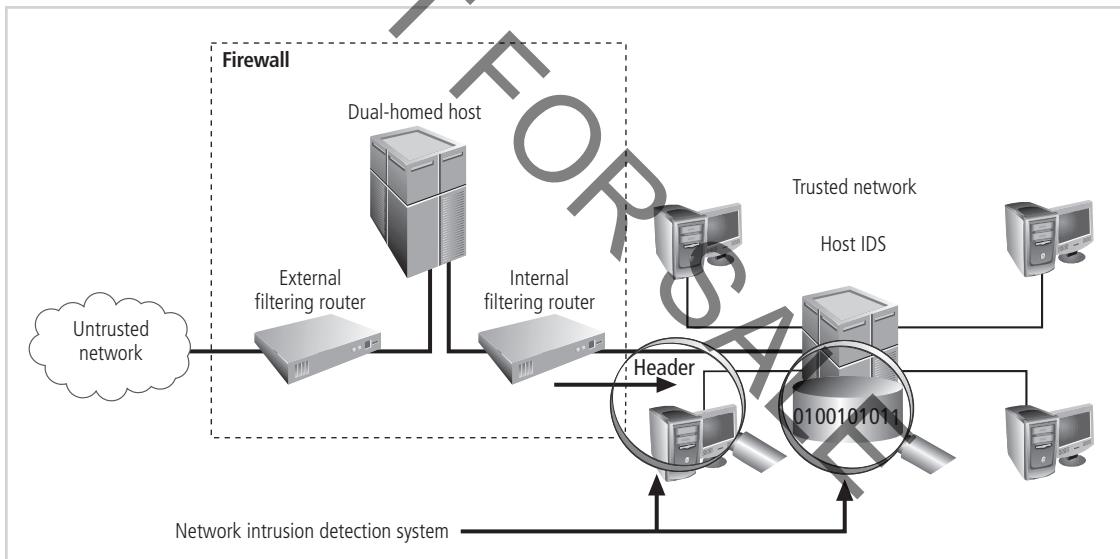


**FIGURE 3-4** Spheres of Security

Information security is designed and implemented in three layers: policies, people (education, training, and awareness programs), and technology. While the design and implementation of the people layer and the technology layer overlap, both must follow the sound management policies discussed earlier in this chapter. Each of the layers contain controls and safeguards that protect the valuable information and information system assets. But before any technical controls or other safeguards are put into place, the policies defining the management philosophies that guide the security process must already be in place.

## Defense in Depth

One of the basic tenets of security architectures is the layered implementation of security. This layered approach is called **defense in depth**. To achieve defense in depth, an organization must establish multiple layers of security controls and safeguards, which can be organized into policy, training and education, and technology, as per the NSTISSC model presented in Chapter 1. While policy itself may not prevent attacks, it certainly prepares the organization to handle them, and coupled with other layers, it can deter attacks. This is true of training and education, which can also provide some defense against attacks stemming from employee ignorance and social engineering. Technology is also implemented in layers, with detection equipment working in tandem with reaction technology, all operating behind access control mechanisms. Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of information is referred to as **redundancy**. Redundancy can be implemented at a number of points throughout the security architecture, such as firewalls, proxy servers, and access controls. Figure 3-5 illustrates the concept of building controls in multiple, sometimes redundant layers. The figure shows the use of firewalls and intrusion detection systems (IDS) that use both packet-level rules (shown as the header in the diagram) and data content analysis (shown as 0100101011 in the diagram).

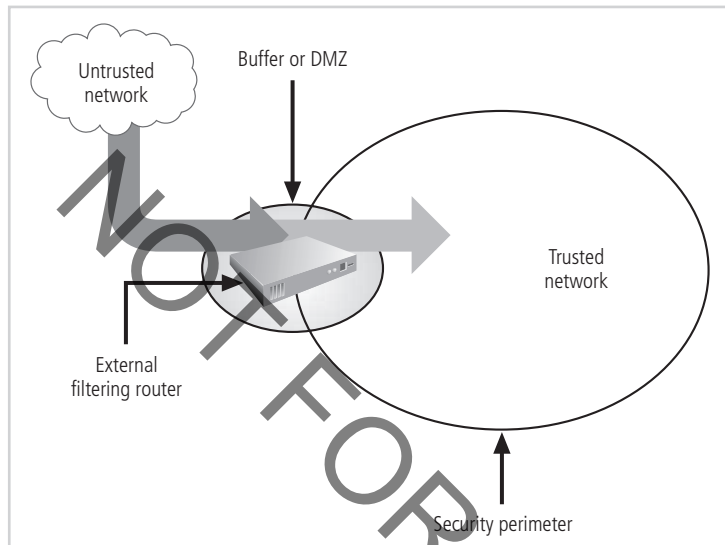


**FIGURE 3-5** Defense in Depth

## Security Perimeter

A **security perimeter** defines the boundary between the outer limit of an organization's security and the beginning of the outside world. A security perimeter protects all internal systems from outside threats, as pictured in Figure 3-6. Unfortunately, the perimeter does not protect against internal attacks from employee threats or on-site physical threats. There can be both an electronic security perimeter, usually at the organization's exterior network or Internet connection, and a physical security perimeter, usually at the gate to the organization's offices. Both require perimeter security. Security perimeters can be implemented as multiple technologies that segregate the protected information from

potential attackers. Within security perimeters the organization can establish **security domains**, or areas of trust within which users can freely communicate. The assumption is that if individuals have access to one system within a security domain, they have authorized access to all systems within that particular domain. The security perimeter is an essential element of the overall security framework, and its implementation details are the core of the completed security blueprint. The key components used for planning the perimeter include firewalls, DMZs, proxy servers, and intrusion detection systems.



**FIGURE 3-6** Security Perimeter

It should be noted that the proliferation of endpoints such as mobile devices are challenging the traditional definition of an organization's perimeter.<sup>13</sup> Enterprises must carefully consider how these new technologies can redefine where the perimeter actually falls.

## Security Education, Training, and Awareness Program

Once your organization has defined the policies that will guide its security program, selected an overall security model by creating or adapting a security framework, and established a corresponding detailed blueprint for implementation, it is time to implement a **security education, training, and awareness (SETA)** program. The SETA program is the responsibility of the CISO and is a control measure designed to reduce the incidences of accidental security breaches by employees. Employee errors are among the top threats to information assets, so it is worth expending the organization's resources to develop programs to combat this threat. SETA programs are designed to supplement the general education and training programs that many organizations have in place to educate staff on information security. For example, if an organization detects that many employees are opening e-mail attachments inappropriately, those employees must be retrained. As a matter of good practice, systems development life cycles must include user training during the implementation phase.

The SETA program consists of three elements: security education, security training, and security awareness. An organization may not be able or willing to undertake all three of these elements; in this case, it may outsource elements to local educational institutions. The purpose of SETA is to enhance security by:

- Improving awareness of the need to protect system resources
- Developing skills and knowledge so computer users can perform their jobs more securely
- Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems<sup>14</sup>

Table 3-6 compares the features of security education, training, and awareness within the organization.

**TABLE 3-6** Comparative Framework of SETA (from NIST SP800-12<sup>15</sup>)

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching method	Theoretical instruction • Discussion seminar • Background reading • Hands-on practice	Practical instruction • Lecture • Case study workshop • Posters	Media • Videos • Newsletters
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long-term	Intermediate	Short-term

## Security Education

Everyone in an organization needs to be trained and made aware of information security, but not every member of the organization needs a formal degree or certification in information security. When management agrees that formal education is appropriate, an employee can investigate available courses from local institutions of higher learning or continuing education. A number of universities have formal coursework in information security. Those interested in researching formal information security programs can use resources such as the NSA-identified National Centers of Academic Excellence in Information Assurance Education ([www.nsa.gov/ia/academia/caemap.cfm?MenuID=10.1.1.2](http://www.nsa.gov/ia/academia/caemap.cfm?MenuID=10.1.1.2)). The Centers of Excellence program identifies outstanding universities with both coursework in information security and an integrated view of information security in the institution itself. Other local resources can also provide security education information, such as Kennesaw State's Center for Information Security Education (<http://infosec.kennesaw.edu>).

## Security Training

Security training provides detailed information and hands-on instruction to employees to prepare them to perform their duties securely. Management of information security can develop customized in-house training or outsource the training program.

Alternatives to formal training programs are industry training conferences and programs offered through professional agencies such as SANS ([www.sans.org](http://www.sans.org)), ISC<sup>2</sup> ([www.isc2.org](http://www.isc2.org)), ISSA ([www.issa.org](http://www.issa.org)), and CSI ([www.gocsi.com](http://www.gocsi.com)). Many of these programs are too technical for the average employee, but may be perfect for the continuing education requirements of information security professionals.

A number of SETA resources offer assistance in the form of sample topics and structures for security classes. The Computer Security Resource Center at NIST provides several useful documents free of charge in their special publications area (<http://csrc.nist.gov>).

## Security Awareness

One of the least frequently implemented but most beneficial programs is the security awareness program. A security awareness program is designed to keep information security at the forefront of users' minds. These programs don't have to be complicated or expensive. Good programs can include newsletters, security posters (see Figure 3-7 for an example), videos, bulletin boards, flyers, and trinkets. Trinkets can include security slogans printed on mouse pads, coffee cups, T-shirts, pens, or any object frequently used during the workday that reminds employees of security. In addition, a good security awareness program requires a dedicated individual willing to invest the time and effort into promoting the program, and a champion willing to provide the needed financial support.



**FIGURE 3-7** Example Security Awareness Poster

The security newsletter is the most cost-effective method of disseminating security information and news to the employee. Newsletters can be distributed via hard copy, e-mail, or intranet. Newsletter topics can include information about new threats

to the organization's information assets, the schedule for upcoming security classes, and security personnel updates. The goal is to keep the idea of information security in users' minds and to stimulate users to care about security. If a security awareness program is not actively implemented, employees may begin to neglect security matters and the risk of employee accidents and failures is likely to increase.

## Continuity Strategies

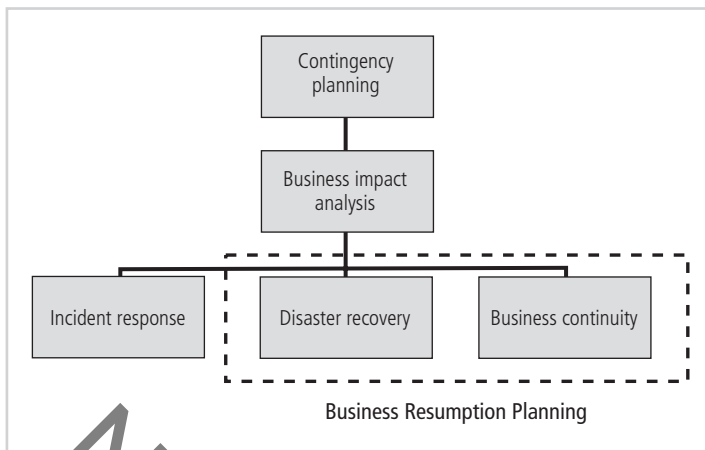
A key role for all managers is planning. Managers in the IT and information security communities are usually called on to provide strategic planning to ensure the continuous availability of information systems.<sup>16</sup> Unfortunately for managers, however, the probability that some form of attack will occur, whether from inside or outside, intentional or accidental, human or nonhuman, annoying or catastrophic, is very high. Thus, managers from each community of interest within the organization must be ready to act when a successful attack occurs.

There are various types of plans for events of this type: business continuity (BC) plans, disaster recovery (DR) plans, incident response (IR) plans, and contingency plans. In some organizations, these might be handled as a single integrated plan. In large, complex organizations, each of these plans may cover separate but related functions that differ in scope, applicability, and design. In a small organization, the security administrator (or systems administrator) may have one simple plan that consists of a straightforward set of media backup and recovery strategies, and a few service agreements from the company's service providers. But the sad reality is that many organizations have a level of planning that is woefully deficient.

Incident response, disaster recovery, and business continuity planning are components of contingency planning, as shown in Figure 3-8. A **contingency plan** is prepared by the organization to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization, and, subsequently, to restore the organization to normal modes of business operations. The discussion of contingency planning begins with an explanation of the differences among its various elements, and an examination of the points at which each element is brought into play.

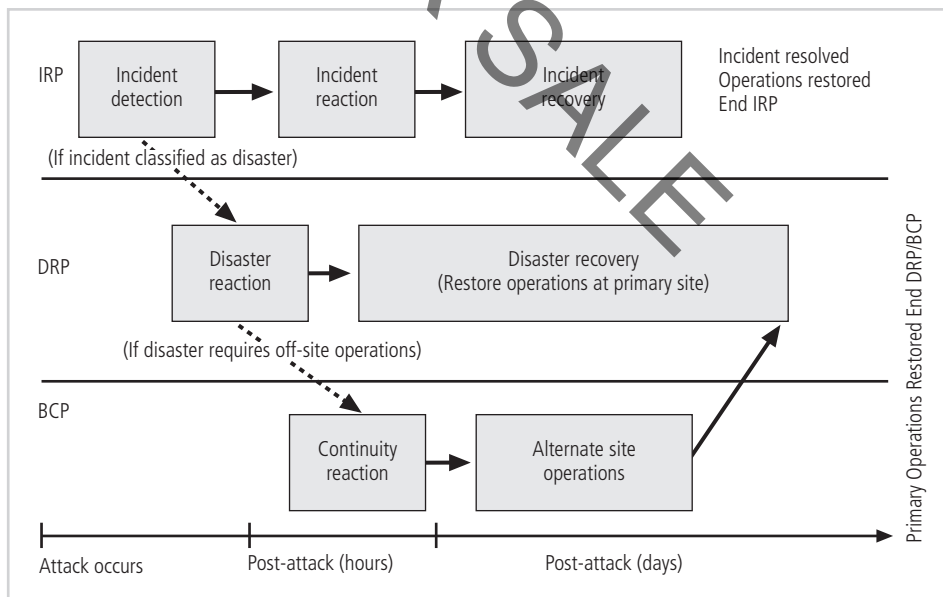
An **incident** is any clearly identified attack on the organization's information assets that would threaten the assets' confidentiality, integrity, or availability. An **incident response (IR) plan** addresses the identification and classification of, response to, and recovery from an incident. A **disaster recovery (DR) plan** addresses the preparation for and recovery from a disaster, whether natural or man-made. A **business continuity (BC) plan** ensures that critical business functions continue, if a catastrophic incident or disaster occurs. The primary functions of these three types of planning are as follows:

- The IR plan focuses on immediate response, but if the attack escalates or is disastrous (e.g., fire, flood, earthquake, or total blackout), the process moves on to the disaster recovery and BC plans.
- The DR plan typically focuses on restoring systems at the original site after disasters occur, and as such is closely associated with BC plan.
- The BC plan occurs concurrently with DR plan when the damage is major or long-term, requiring more than simple restoration of information and information resources. The BC plan establishes critical business functions at an alternate site.



**FIGURE 3-8** Components of Contingency Planning

Some experts argue that the DR plans and BC plans are so closely linked that they are indistinguishable. However, each has a distinct role and planning requirement. The following sections detail the tasks necessary for each of these three types of plans. You can also further distinguish the three types of planning by examining when each comes into play during the life of an incident. Figure 3-9 shows a sample sequence of events and the overlap between when each plan comes into play. Disaster recovery activities typically continue even after the organization has resumed operations at the original site.



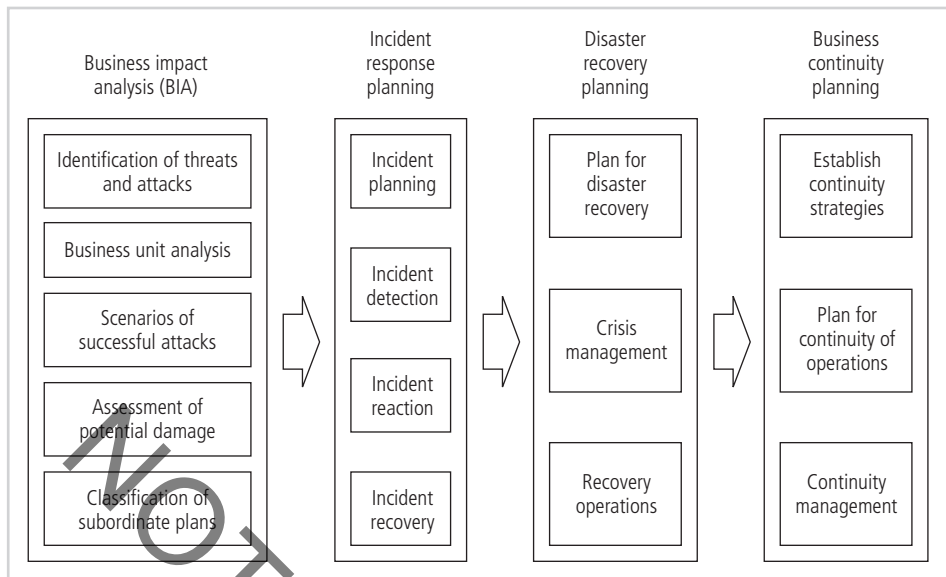
**FIGURE 3-9** Contingency Planning Timeline

Contingency planning is similar to another process—one that you may have heard about and are likely to encounter in your education or future employment—called the risk management process. The contingency plan is a microcosm of risk management activities, and it focuses on the specific steps that must be taken to restore all information assets to their pre-incident or disaster states. As a result, the planning process closely emulates the risk management process.

Before any planning can begin, an assigned person or a planning team must begin the process. Typically, a contingency planning team is assembled for that purpose. A roster for this team may consist of the following members:

- **Champion**—As with any strategic function, the contingency planning project must have a high-level manager to support, promote, and endorse the findings of the project. In a contingency planning project, this could be the CIO, or ideally the CEO.
- **Project manager**—A project manager, possibly a mid-level manager or even the CISO, must lead the project and make sure a sound project-planning process is used, a complete and useful project plan is developed, and project resources are prudently managed to reach the goals of the project.
- **Team members**—The team members for this project should be the managers or their representatives from the various communities of interest: business, information technology, and information security. Representative business managers, familiar with the operations of their respective functional areas, should supply details on their activities and provide insight into the criticality of their functions to the overall sustainability of the business. Information technology managers on the project team should be familiar with the systems that could be at risk and with the IR plans, DR plans, and BC plans that are needed to provide technical content within the planning process. Information security managers must oversee the security planning of the project and provide information on the threats, vulnerabilities, attacks, and recovery requirements needed in the planning process.

The major project work modules performed by the contingency planning project team are shown in Figure 3-10. As you read the remainder of this chapter, it may help you to return to this diagram, since many of the upcoming sections correspond to the steps depicted in the diagram.



**FIGURE 3-10** Major Steps in Contingency Planning

## Business Impact Analysis

The first phase in the development of the contingency planning process is the **business impact analysis (BIA)**. A BIA is an investigation and assessment of the impact that various attacks can have on the organization. BIA takes up where the risk assessment process leaves off. It begins with a prioritized list of threats and vulnerabilities and adds information about the criticality of the systems involved and detailed assessments of the threats and vulnerabilities in the context in which the systems are used. The BIA is a crucial component of the initial planning stages, as it provides detailed analyses of the potential impact each attack could have on the organization. The BIA therefore adds insight into what the organization must do to respond to the attack, minimize the damage from the attack, recover from the effects, and return to normal operations. One of the fundamental differences between a BIA and the risk management processes is that the risk management approach identifies the threats, vulnerabilities, and attacks to determine what controls can protect the information. The BIA assumes that these controls have been bypassed, have failed, or have proven otherwise ineffective, that an attack has succeeded, and attempts to answer the question, *what do you do then?*

The contingency planning team conducts the BIA in the following stages, which are shown in Figure 3-10 and described in the sections that follow:

1. Threat attack identification and prioritization
2. Business unit analysis
3. Attack success scenario development
4. Potential damage assessment
5. Subordinate plan classification

## Threat Attack Identification and Prioritization

Organizations that have a well-established risk management process will not need to develop this aspect of the BIA and need only to update the threat list from their risk management process with new developments and add one additional piece of information, the attack profile. An **attack profile** is a detailed description of the activities that occur during an attack. The content items in an attack profile, shown in Table 3-7, include preliminary indications of an attack, as well as actions and outcomes. These profiles must be developed for every serious threat the organization faces, natural or man-made, deliberate or accidental. It is as important to know the typical hacker's profile as it is to know what kind of data entry mistakes employees make, or the weather conditions that indicate an imminent tornado or hurricane. The attack profile is useful in later planning stages to provide indicators of attacks. It is used here to determine the extent of damage that could result to a business unit if a given attack were successful.

**TABLE 3-7** Attack Profile

Date of analysis	June 21, 2008
Attack name and description	Mako worm
Threat and probable threat agent	Malicious code via automated attack
Known or possible vulnerabilities	All desktop systems not updated with all latest patches
Likely precursor activities or indicators	Attachments to e-mails
Likely attack activities or indicators of attack in progress	Systems sending e-mails to entries from address book, activity on port 80 without browser being used
Information assets at risk from this attack	All desktop and server systems are at risk
Damage or loss to information assets likely from this attack	Business partners and others connected to our networks
Other assets at risk from this attack	None identified at this time
Damage or loss to other assets likely from this attack	Will vary depending on severity, minimum disruption will be needed to repair worm infection

## Business Unit Analysis

The second major task within the BIA is the analysis and prioritization of the business functions within the organization's departments, sections, divisions, groups, or other units to determine which are most vital to continued operations. Each unit must also be evaluated to determine how important its functions are to the organization as a whole. For example, recovery operations would probably focus on the IT department and network operation before addressing the personnel department and hiring activities. Likewise, it is more urgent to reinstate a manufacturing company's assembly line than the maintenance tracking system for that assembly line. This is not to say that personnel functions and assembly line maintenance are not important to the business; however, the reality is that if the organization's main revenue-producing operations cannot be restored quickly, there may cease to be a need for other functions.

### Attack Success Scenario Development

Once the threat attack profiles have been developed and the business functions prioritized, the business impact analysis team must create a series of scenarios depicting the impact of a successful attack from each threat on each prioritized functional area. This can be a long and detailed process, as threats that succeed can affect many functions. Attack profiles should include scenarios depicting a typical attack with details on the method, the indicators, and the broad consequences of the attack. Once the attack profiles are completed, the business function details can be integrated with the attack profiles, after which more details are added to the attack profile, including alternate outcomes. These alternate outcomes should describe a best, worst, and most likely case that could result from each type of attack on a particular business functional area. This level of detail allows planners to address each business function in turn.

### Potential Damage Assessment

Using the attack success scenarios, the BIA planning team must estimate the cost of the best, worst, and most likely cases. At this stage, you are *not* determining how much to spend on the protection of information assets, rather, you are identifying what must be done to recover from each possible case. These costs include the actions of the response team(s), which are described in subsequent sections, as they act to recover quickly and effectively from an incident or disaster. These cost estimates can also inform management representatives from all the organization's communities of interest of the importance of the planning and recovery efforts. The final result of the assessment is referred to as an **attack scenario end case**.

### Subordinate Plan Classification

Once the potential damage has been assessed, and each scenario and attack scenario end case has been evaluated, a subordinate plan must be developed or identified from among existing plans already in place. These subordinate plans take into account the identification of, reaction to, and recovery from each attack scenario. An attack scenario end case is categorized either as disastrous or not disastrous. Most attacks are not disastrous and therefore fall into the category of incident. Those scenarios that do qualify as disastrous are addressed in the disaster recovery plan. The qualifying difference is whether or not an organization is able to take effective action during the attack to combat its effects. Attack end cases that are disastrous find members of the organization waiting out the attack with hopes to recover effectively after it is over. In a typical disaster recovery operation, the lives and welfare of the employees are the most important priority *during* the attack, as most disasters are fires, floods, hurricanes, and tornadoes. Please note that there are attacks that are not natural disasters that fit this category as well, for example:

- Electrical blackouts
- Attacks on service providers that result in a loss of communications to the organization (either telephone or Internet)
- Massive, malicious code attacks that sweep through an organization before they can be contained

The objective of this process is that each scenario should be classified as a probable incident or disaster, and then the corresponding actions required to respond to the scenario should be built into either the IR plan or DR plan.

## Incident Response Planning

Incident response planning includes the identification of, classification of, and response to an incident. The IR plan is made up of activities that are to be performed when an incident has been identified. Before developing such a plan, you should understand the philosophical approach to incident response planning.

What is an incident? What is incident response? As stated earlier, an incident is an attack against an information asset that poses a clear threat to the confidentiality, integrity, or availability of information resources. If an action that threatens information is confirmed, the action is classified as an incident. All of the threats identified in earlier chapters could result in attacks that would be classified as information security incidents. For purposes of this discussion, however, attacks are only classified as incidents if they have the following characteristics:

- They are directed against information assets.
- They have a realistic chance of success.
- They could threaten the confidentiality, integrity, or availability of information resources.

**Incident response (IR)** is therefore the set of activities taken to plan for, detect, and correct the impact of an incident on information assets. Prevention is purposefully omitted, as this activity is more a function of information security in general than of incident response. In other words, IR is more reactive than proactive, with the exception of the planning that must occur to prepare the IR teams to be ready to react to an incident.

IR consists of the following four phases:

1. Planning
2. Detection
3. Reaction
4. Recovery

## Disaster Recovery Planning

An event can be categorized as a disaster when the following happens: (1) the organization is unable to mitigate the impact of an incident during the incident, and (2) the level of damage or destruction is so severe that the organization is unable to recover quickly. The difference between an incident and a disaster may be subtle; the contingency planning team must make the distinction between disasters and incidents, and it may not be possible to make this distinction until an attack occurs. Often an event that is initially classified as an incident is later determined to be a disaster. When this happens, the organization must change how it is responding and take action to secure its most valuable assets to preserve value for the longer term, even at the risk of more disruption in the short term.

Disaster recovery (DR) planning is the process of preparing an organization to handle and recover from a disaster, whether natural or man-made. The key emphasis of a DR plan is to reestablish operations at the primary site, the location at which the organization performs its business. The goal is to make things whole, or as they were before the disaster.

## The Disaster Recovery Plan

Similar in structure to the IR plan, the DR plan provides detailed guidance in the event of a disaster. It is organized by the type or nature of the disaster, and specifies recovery procedures during and after each type of disaster. It also provides details on the roles and responsibilities of the people involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified. Just as the IR plan must be tested, so must the DR plan, using the same testing mechanisms. At a minimum, the DR plan must be reviewed during a walk-through or talk-through on a periodic basis.

Many of the same precepts of incident response apply to disaster recovery:

1. Priorities must be clearly established. The first priority is always the preservation of human life. The protection of data and systems immediately falls to the wayside if the disaster threatens the lives, health, or welfare of the employees of the organization or members of the community in which the organization operates. Only after all employees and neighbors have been safeguarded can the disaster recovery team attend to nonhuman asset protection.
2. Roles and responsibilities must be clearly delineated. Everyone assigned to the DR team should be aware of his or her expected actions during a disaster. Some people are responsible for coordinating with local authorities, such as fire, police, and medical staff. Others are responsible for the evacuation of personnel, if required. Still others are tasked simply to pack up and leave.
3. Someone must initiate the alert roster and notify key personnel. Those to be notified may be the fire, police, or medical authorities mentioned earlier. They may also include insurance agencies, disaster teams like the Red Cross, and management teams.
4. Someone must be tasked with the documentation of the disaster. Just as in an IR reaction, someone must begin recording what happened to serve as a basis for later determination of why and how the event occurred.
5. If and only if it is possible, attempts must be made to mitigate the impact of the disaster on the operations of the organization. If everyone is safe, and all needed authorities have been notified, some individuals can be tasked with the evacuation of physical assets. Some can be responsible for making sure all systems are securely shut down to prevent further loss of data.

## Recovery Operations

Reaction to a disaster can vary so widely that it is impossible to describe the process with any accuracy. Each organization must examine the scenarios developed at the start of contingency planning, and determine how to respond.

If the physical facilities are spared, the disaster recovery team should begin the restoration of systems and data to reestablish full operational capability. If the organization's facilities do not survive, alternative actions must be taken until new facilities can be acquired. When a disaster threatens the viability of the organization at the primary site, the disaster recovery process transitions into the process of business continuity planning.

## Business Continuity Planning

**Business continuity planning** prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site. If a disaster has rendered the current location unusable, there must be a plan to allow the business to

continue to function. Not every business needs such a plan or such facilities. Small companies or fiscally sound organizations may have the latitude to cease operations until the physical facilities can be restored. But organizations such as manufacturers and retailers may not have this option, because they depend on physical types of commerce and may not be able to relocate operations.

### Developing Continuity Programs

Once the incident response plans and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support the continued viability of the business in the event of a disaster. The development of the BC plan is somewhat simpler than that of the IR plan or DR plan, in that it consists primarily of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy. Some of the components of the BC plan could already be integral to the normal operations of the organization, such as an off-site backup service. Others require special consideration and negotiation. The first part of business continuity planning is performed when the joint DR/BC plan is developed. The identification of critical business functions and the resources needed to support them is the cornerstone of the BC plan. When a disaster strikes, these functions are the first to be reestablished at the alternate site. The contingency planning team needs to appoint a group of individuals to evaluate and compare the available alternatives, and recommend which strategy should be selected and implemented. The strategy selected usually involves some form of off-site facility, which should be inspected, configured, secured, and tested on a periodic basis. The selection should be reviewed periodically to determine if a superior alternative has emerged or if the organization needs a different solution.

### Crisis Management

Disasters are, of course, larger in scale and less manageable than incidents, but the planning processes are the same, and in many cases are conducted simultaneously. What may truly distinguish an incident from a disaster is the actions of the response teams. An incident response team typically rushes to duty stations or to the office from home. The first act is to reach for the IR plan. A disaster recovery team may not have the luxury of flipping through a binder to see what must be done. Disaster recovery personnel must know their roles without any supporting documentation. This is a function of preparation, training, and rehearsal. You probably all remember the frequent fire, tornado, or hurricane drills—and even the occasional nuclear blast drills—from your public school days. Fire or disaster is no less likely in the business world.

The actions taken during and after a disaster are referred to as **crisis management**. Crisis management differs dramatically from incident response, as it focuses first and foremost on the people involved. It also addresses the viability of the business. The disaster recovery team works closely with the crisis management team. According to Gartner Research, the crisis management team is

responsible for managing the event from an enterprise perspective and covers the following major activities:

- Supporting personnel and their loved ones during the crisis
- Determining the event's impact on normal business operations and, if necessary, making a disaster declaration

- Keeping the public informed about the event and the actions being taken to ensure the recovery of personnel and the enterprise
- Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties.<sup>17</sup>

The crisis management team should establish a base of operations or command center to support communications until the disaster has ended. The crisis management team includes individuals from all functional areas of the organization, to facilitate communications and cooperation. Some key areas of crisis management include:

- Verifying personnel head count: Everyone must be accounted for, including those on vacations, leaves of absence, and business trips.
- Checking the alert roster: Alert rosters and general personnel phone lists are used to notify individuals whose assistance may be needed, or simply to tell employees not to report to work until the disaster is over.
- Checking emergency information cards: It is important that each employee have two types of emergency information cards. The first is personal emergency information that specifies whom to notify in case of an emergency (next of kin), medical conditions, and a photocopy of the employee's driver's license or other identification. The second is a set of instructions on what to do in the event of an emergency. This mini-snapshot of the disaster recovery plan should contain, at a minimum, a contact number or hot line, emergency services numbers (fire, police, medical), evacuation and assembly locations (storm shelters, for example), the name and number of the disaster recovery coordinator, and any other needed information.

Crisis management must balance the needs of the employees with the needs of the business in providing personnel with support for personal and family issues during disasters.

---

## Chapter Summary

- In order to most effectively secure its networks, an organization must establish a functional and well-designed information security program in the context of a well-planned and fully defined information policy and planning environment. The creation of an information security program requires information security policies, standards and practices, an information security architecture, and a detailed information security blueprint.
- Management must make policy the basis for all information security planning, design, and deployment in order to direct how issues are addressed and how technologies are used. Policy must never conflict with laws, but should stand up in court, if challenged, and should be properly administered through dissemination and documented acceptance. For a policy to be considered effective and legally enforceable, it must be disseminated, reviewed, understood, complied with, and uniformly enforced. Policy is implemented with an overall enterprise information security policy and as many issue-specific and system-specific policies as are indicated to meet the management team's policy needs.

- After the information security team identifies the vulnerabilities in the information technology systems, the security team develops a design blueprint for security used to implement the security program. The security blueprint is a detailed version of the security framework, an outline of steps to take to design and implement information security in the organization. There are a number of published information security frameworks, but since each information security environment is unique, the security team may need to modify or adapt pieces from several frameworks.
- Each organization should implement a security education, training, and awareness (SETA) program to supplement the general education and training programs that many organizations have in place to educate staff on information security. A SETA program consists of three elements: security education, security training, and security awareness. The purpose of SETA is to enhance security by: improving awareness of the need to protect system resources, developing skills and knowledge so computer users can perform their jobs more securely, and building in-depth knowledge to design, implement, or operate security programs for organizations and systems.
- Managers in the IT and information security communities must ensure the continuous availability of information systems. This is achieved with various types of contingency planning such as: incident response, disaster recovery, and business continuity planning. An incident response (IR) plan addresses the identification and classification of, response to, and recovery from an incident. A disaster recovery (DR) plan addresses the preparation for and recovery from a disaster, whether natural or man-made. A business continuity (BC) plan ensures that critical business functions continue, if a catastrophic incident or disaster occurs.

---

## Review Questions

1. What is management's role with regard to information security policies and practices?
2. What are the differences between a policy, a standard, and a practice? What are the three types of security policies? Where would each be used? What type of policy would be needed to guide use of the Web? E-mail? Office equipment for personal use?
3. For a policy to be considered effective and legally enforceable, what must it accomplish?
4. What are the components of an effective EISP?
5. What are the components of an effective ISSP?
6. What is an ACL and how does it fit into the discussion about policy? Hint: look at the SysSP.
7. Who is ultimately responsible for managing a technology? Who is responsible for enforcing policy that affects the use of a technology?
8. What must occur for a security policy to remain viable?
9. What is the difference between a security framework and a security blueprint?
10. How can a security framework assist in the design and implementation of a security infrastructure?
11. Where can a security administrator find information on established security frameworks?
12. What is the ISO 27000 series of standards? What individual standards make up the series?
13. Briefly describe the history of the standard now known as ISO 27002. In which country did it originate? Has it had any other names?
14. What documents are available from the NIST Computer Resource Center, and how can they support the development of a security framework?
15. Define benchmarking. What is it used for?

16. Briefly describe the spheres of security. Who could benefit from understanding this approach to security?
17. What is defense in depth? Why is this so often encountered in information security technical control settings?
18. What resources are available on the Web that can aid an organization in developing best practices as part of a security framework?
19. What is SETA? Which organizations should have a SETA program?
20. What is contingency planning? How is it different from routine management planning?
21. What are the components of contingency planning, and what are the major steps used for contingency planning?
22. When is IR planning used?
23. When is DR planning used?
24. When is BC planning used? How do you determine when to use the IR plan, DR plan, or BC plan?
25. What are the elements of a business impact analysis?

---

## Exercises

1. Using a graphics program, design several security awareness posters on the following themes: updating antivirus signatures, protecting sensitive information, watching out for e-mail viruses, prohibiting the personal use of company equipment, changing and protecting passwords, avoiding social engineering, and protecting software copyrights. What other areas can you come up with?
2. Search the Web for a listing of security education and training programs in your area. Keep a list and see which category has the most examples. See if you can determine the costs associated with each example. Which do you feel would be more cost-effective in terms of both time and money?
3. Search the Web for examples of issue-specific security policies. What types of policies can you find? Draft a simple issue-specific policy using the format provided in the text that outlines "Fair and Responsible Use of College Computers" and is based on the rules and regulations you have been provided with in your institution. Does your school have a similar policy? Does it contain all the elements listed in the text?
4. Use your library or the Web to find a reported natural disaster that occurred within the last 180 days. From the news accounts, determine if local or national officials had prepared disaster plans and if these plans were used. See if you can determine how the plans helped the officials improve the response to the disaster. How do the plans help the recovery?
5. Classify each of the following occurrences as an incident or disaster. If an occurrence is a disaster, determine whether or not business continuity plans would be called into play.
  - a. A hacker gets into the network and deletes files from a server.
  - b. A fire breaks out in the storeroom and sets off sprinklers on that floor. Some computers are damaged, but the fire is contained.
  - c. A tornado hits a local power company, and the company will be without power for three to five days.
  - d. Employees go on strike, and the company could be without critical workers for weeks.
  - e. A disgruntled employee takes a critical server home, sneaking it out after hours.For each of the scenarios (a–e), describe the steps necessary to restore operations. Indicate whether or not law enforcement would be involved.

## Case Exercises

Matthias and Al watched the monitor for a few more minutes. The firewall at *Linen Planet* seemed to be running just fine.

Al stood up and went on to his next task, and Matthias also moved on to his next task. After an hour, he picked up the phone and called the number for the QA team.

"Hello, QA Test Team, Debbie speaking."

"Hi Debbie," said Matthias. "What's the word on the Linen Planet firewall project?"

"Oh, we just finished," said Debbie. "We're good to go. The new rules can stay in place."

Matthias said, "OK. We won't roll back. Thanks for the info."

Debbie replied, "OK. I'll put a note on the test log. Thanks for your help."

They both hung up the phone. As Al walked across the room, Matthias called out to him, "Is it always this easy?"

Al shook his head. "Not hardly, you must be having beginner's luck."

### Questions:

1. What are some of the things that might have gone wrong in the test?
2. If the test had failed, what do you think the rollback plan would have entailed?
3. What is the relationship between the EISP, the network usage ISSP, and the rules that Matthias entered in the updated firewall?

### Endnotes

1. Charles Cresson Wood. "Integrated Approach Includes Information Security." *Security* 37, no. 2 (February 2000): 43–44.
2. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. SP 800-12.
3. Derived from a number of sources, the most notable of which is [www.wustl.edu/policies/infosecurity.html](http://www.wustl.edu/policies/infosecurity.html).
4. Robert J. Alberts, Anthony M. Townsend, and Michael E. Whitman. "Considerations for an Effective Telecommunications Use Policy." *Communications of the ACM* 42, no. 6 (June 1999): 101–109.
5. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. SP 800-12.
6. National Institute of Standards and Technology. *Information Security Management, Code of Practice for Information Security Management*. ISO/IEC 17799 (6 December 2001).
7. National Institute of Standards and Technology. *Information Security Management, Code of Practice for Information Security Management*. ISO/IEC 17799 (6 December 2001).
8. National Institute of Standards and Technology. *Information Security Management, Code of Practice for Information Security Management*. ISO/IEC 17799 (6 December 2001).
9. National Institute of Standards and Technology. *Information Security Management, Code of Practice for Information Security Management*. ISO/IEC 17799 (6 December 2001).
10. T. Humphries. The Newly Revised Part 2 of BS 7799. Accessed May 27, 2003. [www.gammasl.co.uk/bs7799/The%20Newly%20Revised%20Part%202%20of%20BS%207799ver3a.pdf](http://www.gammasl.co.uk/bs7799/The%20Newly%20Revised%20Part%202%20of%20BS%207799ver3a.pdf).
11. How 7799 Works. WWW Document [Cited 27 May, 2003] available from [www.gammasl.co.uk/bs7799/works.html](http://www.gammasl.co.uk/bs7799/works.html).

12. Kadrich, M. *Endpoint Security* (Boston: Addison-Wesley, 2007).
13. National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*. SP 800-12.
14. National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*. SP 800-12.
15. William R. King and Paul Gray, *The Management of Information Systems* (Chicago: Dryden Press, 1989), 359.
16. Roberta Witty, "What Is Crisis Management?" *Gartner Online* (19 September 2001). Accessed 30 April, 2007 from [www.gartner.com/DisplayDocument?id=340971](http://www.gartner.com/DisplayDocument?id=340971).

NOT FOR SALE

NOT FOR SALE