CHAPTER 17

# IT Security Controls, Plans, and Procedures


17.1 **IT Security Management Implementation**

17.2 **Security Controls or Safeguards**

17.3 **IT Security Plan**

17.4 **Implementation of Controls**

- Implementation of Security Plan
- Security Training
- Security Awareness

17.5 **Implementation Follow-up**

- Maintenance
- Security Compliance
- Change and Configuration Management
- Incident Handling

17.6 **Case Study: Silver Star Mines**

17.7 **Recommended Reading**

17.8 **Key Terms, Review Questions, and Problems**

- Key Terms
- Review Questions
- Problems

In Chapter 16 we introduced IT security management as a formal process to ensure that critical assets are sufficiently protected in a cost-effective manner. We then discussed the critical risk assessment process. This chapter continues the examination of IT security management. We explore the range of management, operational, and technical controls or safeguards available that can be used to improve security of IT systems and processes. We then explore the content of the security plans that detail the implementation process. These plans must then be implemented, with training to ensure that all personnel know their responsibilities, and monitoring to ensure compliance. Finally, to ensure that a suitable level of security is maintained, management must follow up the implementation with an evaluation of the effectiveness of the security controls and an iteration of the entire IT security management process.

## 17.1 IT SECURITY MANAGEMENT IMPLEMENTATION

We introduced the IT security management process in Chapter 16, illustrated by Figure 16.1. Chapter 16 focused on the earlier stages of this process. In this chapter we focus on the latter stages, which include selecting controls, developing an implementation plan, and monitoring the plan's implementation. Details of these steps are illustrated in Figure 17.1 (reproduced from Fig 4-2 in [NIST02]). We discuss each of these broad areas in turn.

## 17.2 SECURITY CONTROLS OR SAFEGUARDS

The results of some form of risk assessment on an organization's IT systems will identify areas needing treatment, and the next step is to select suitable controls to use in this treatment. IT security **controls** or **safeguards** (the two terms are used interchangeably) help to reduce risks. [ISO13335] includes this definition:

> **Safeguards**: are practices, procedures, or mechanisms which may protect against a threat, reduce a vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recovery.

Some controls address multiple risks at the same time, and selecting such controls can be very cost effective. Controls can be classified as belonging to one of the following classes (although some controls include features from several of these):

- **Management control:** Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission. These controls refer to issues that management needs to address.
- **Operational:** Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies. These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems. They are used to improve the security of a system or group of systems.

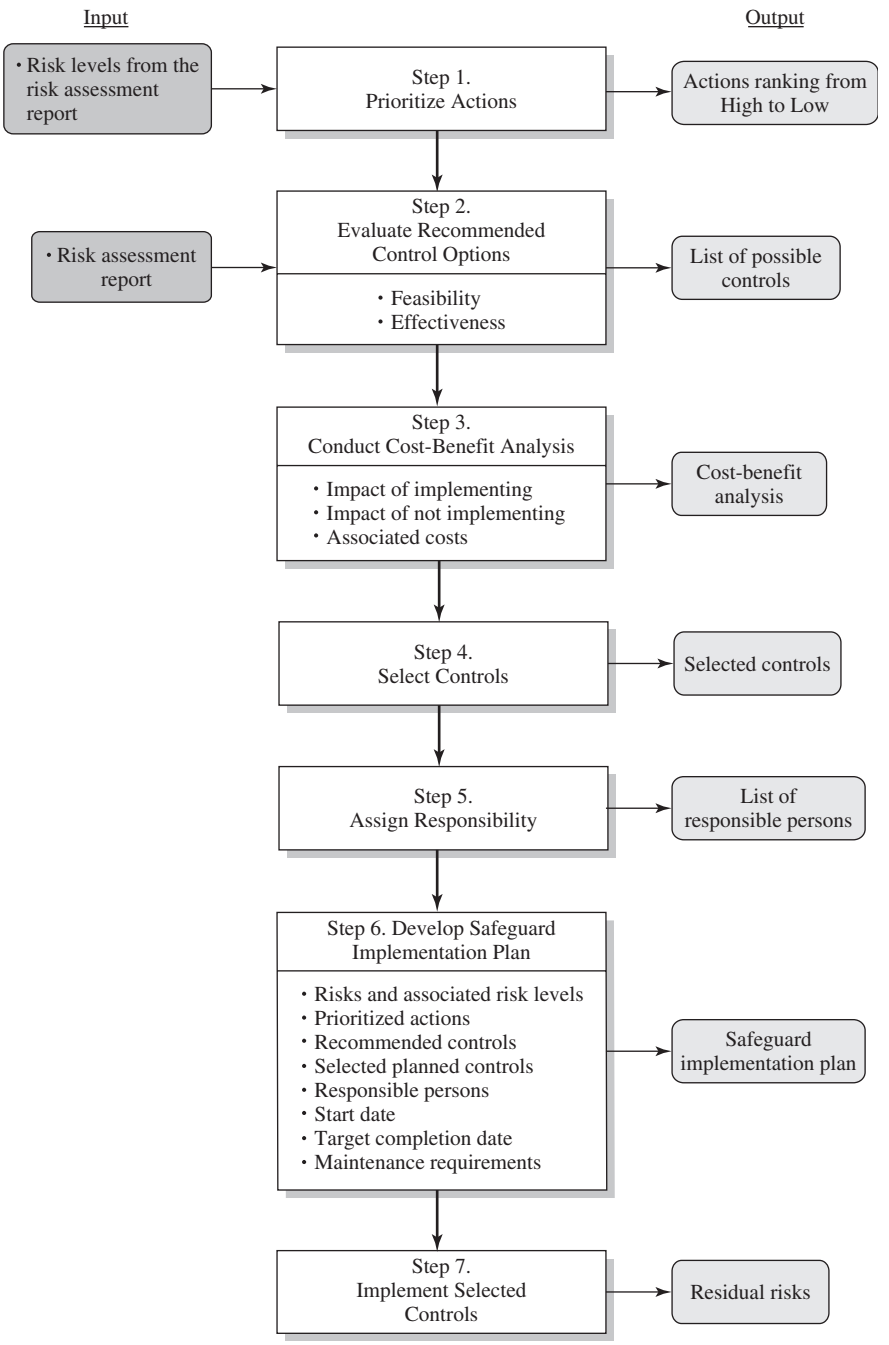


**Figure 17.1 It Security Management Controls and Implementation**

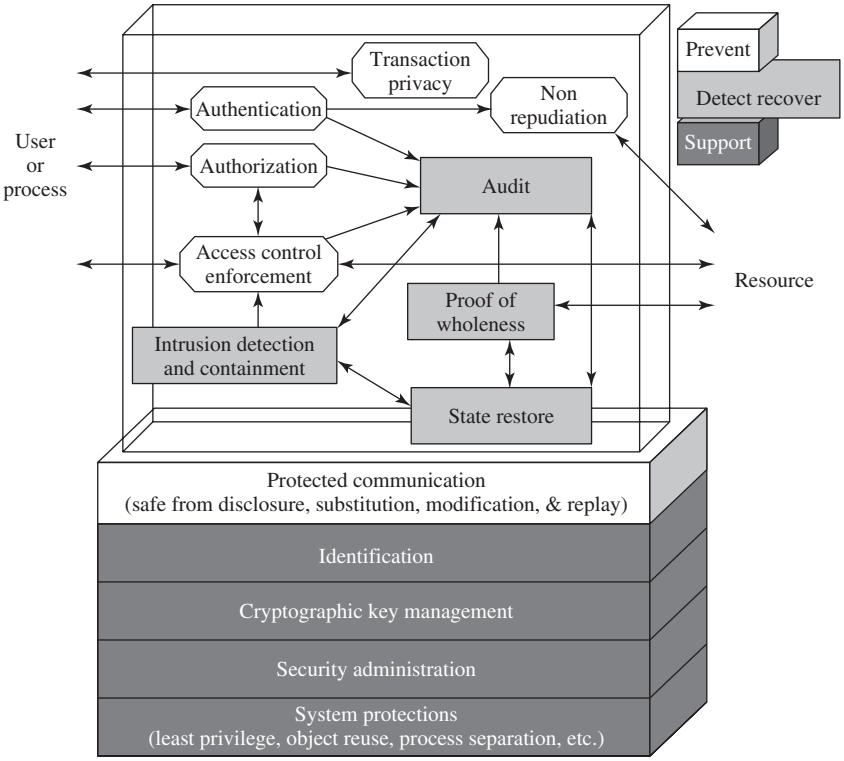


**Figure 17.2 Technical Security Controls**

- **Technical controls:** Involve the correct use of hardware and software security capabilities in systems. These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions. Figure 17.2 (reproduced from Fig 4-3 in [NIST02]) illustrates some typical technical control measures.

In turn, each of these control classes may include the following:

- **Supportive controls:** Pervasive, generic, underlying technical IT security capabilities that are interrelated with, and used by, many other controls.
- **Preventative controls:** Focus on preventing security breaches from occurring, by inhibiting attempts to violate security policies or exploit a vulnerability.
- **Detection and recovery controls:** Focus on the response to a security breach, by warning of violations or attempted violations of security policies or the identified exploit of a vulnerability and by providing means to restore the resulting lost computing resources.

The technical control measures shown in Figure 17.2 include examples of each of these types of controls. Many of these technical controls relate to topics we discuss elsewhere in the text.

Lists of controls are provided in a number of national and international standards, including [ISO17799], [ISO13335], and [NIST05]. There is broad agreement among

**Table 17.1** NIST Security Controls

| Class | Control Family |
|---|---|
| Management | Risk Assessment |
| Management | Planning |
| Management | System and Services Acquisition |
| Management | Certification, Accreditation, and Security Assessments |
| Operational | Personnel Security |
| Operational | Physical and Environmental Protection |
| Operational | Contingency Planning |
| Operational | Configuration Management |
| Operational | Maintenance |
| Operational | System and Information Integrity |
| Operational | Media Protection |
| Operational | Incident Response |
| Operational | Awareness and Training |
| Technical | Identification and Authentication |
| Technical | Access Control |
| Technical | Audit and Accountability |
| Technical | System and Communications Protection |

these and other standards as to the types of controls that should be used and the detailed lists of typical controls. Indeed many of the standards cross-reference each other, indicating their agreement on these lists. [ISO17799] is generally regarded as the master list of controls and is cited by most other standards. Table 17.1 (adapted from table 1 in [NIST05]) is a typical list of families of controls within each of the classes. Compare this with the list in Table 17.2, which details the categories of controls given in [ISO17799], noting the high degree of overlap. Within each of these control classes, there is a long list of specific controls that may be chosen. Table 17.3 (adapted from the table in Appendix D of [NIST05]) itemizes the full list of controls detailed in this standard.

To attain an acceptable level of security, some combination of these controls should be chosen. If the baseline approach is being used, an appropriate baseline set of controls is typically specified in a relevant industry or government standard. For example, Appendix D in [NIST05] lists selections of baseline controls for use in low-, moderate-, and high-impact IT systems. A selection should be made that is appropriate to the organization's overall risk profile, resources, and capabilities. These should then be implemented across all the IT systems for the organization, with adjustments in scope to address broad requirements of specific systems.

**Table 17.2** ISO17799 Security Controls

| Control Categories |
|---|
| Security Policy |
| Organizational Security |
| Asset Classification and Control |
| Personnel Security |
| Physical and Environmental Security |
| Communications and Operations Management |
| Access Control |
| Systems Development and Maintenance |
| Business Continuity Management |
| Compliance |

**Table 17.3** Detailed NIST Security Controls

**Access Control**
Access Control Policy and Procedures, Account Management, Access Enforcement, Information Flow Enforcement, Separation of Duties, Least Privilege, Unsuccessful Login Attempts, System Use Notification, Previous Logon Notification, Concurrent Session Control, Session Lock, Session Termination, Access Control Supervision and Review, Permitted Actions w/o Identification or Authentication, Automated Marking, Automated Labeling, Remote Access, Wireless Access Restrictions, Access Control for Portable and Mobile Systems, Personally Owned Information Systems

**Awareness and Training**
Security Awareness and Training Policy and Procedures, Security Awareness, Security Training, Security Training Records

**Audit and Accountability**
Audit and Accountability Policy and Procedures, Auditable Events, Content of Audit Records, Audit Storage Capacity, Audit Processing, Audit Monitoring, Analysis, and Reporting, Audit Reduction and Report Generation, Time Stamps, Protection of Audit Information, Non-repudiation, Audit Retention

**Certification, Accreditation, and Security Assessments**
Certification, Accreditation, and Security Assessment Policies and Procedures, Security Assessments, Information System Connections, Security Certification, Plan of Action and Milestones, Security Accreditation, Continuous Monitoring

**Configuration Management**
Configuration Management Policy and Procedures, Baseline Configuration, Configuration Change Control, Monitoring Configuration Changes, Access Restrictions for Change, Configuration Settings, Least Functionality

**Contingency Planning**
Contingency Planning Policy and Procedures, Contingency Plan, Contingency Training, Contingency Plan Testing, Contingency Plan Update, Alternate Storage Sites, Alternate Processing Sites, Telecommunications Services, Information System Backup, Information System Recovery and Reconstitution

(*Continued*)

**Table 17.3** (*Continued*)

**Identification and Authentication**
Identification and Authentication Policy and Procedures, User Identification and Authentication, Device Identification and Authentication, Identifier Management, Authenticator Management, Authenticator Feedback, Cryptographic Module Authentication

**Incident Response**
Incident Response Policy and Procedures, Incident Response Training, Incident Response Testing, Incident Handling, Incident Monitoring, Incident Reporting, Incident Response Assistance

**Maintenance**
System Maintenance Policy and Procedures, Periodic Maintenance, Maintenance Tools, Remote Maintenance, Maintenance Personnel, Timely Maintenance

**Media Protection**
Media Protection Policy and Procedures, Media Access, Media Labeling, Media Storage, Media Transport, Media Sanitization Media Destruction and Disposal

**Physical and Environmental Protection**
Physical and Environmental Protection Policy and Procedures, Physical Access Authorizations, Physical Access Control, Access Control for Transmission Medium, Access Control for Display Medium, Monitoring Physical Access, Visitor Control, Access Logs, Power Equipment and Power Cabling, Emergency Shutoff, Emergency Power, Emergency Lighting, Fire Protection, Temperature and Humidity Controls, Water Damage Protection, Delivery and Removal, Alternate Work Site

**Planning**
Security Planning Policy and Procedures, System Security Plan, System Security Plan Update, Rules of Behavior, Privacy Impact Assessment

**Personnel Security**
Personnel Security Policy and Procedures, Position Categorization, Personnel Screening, Personnel Termination, Personnel Transfer, Access Agreements, Third-Party Personnel Security, Personnel Sanctions

**Risk Assessment**
Risk Assessment Policy and Procedures, Security Categorization, Risk Assessment, Risk Assessment Update, Vulnerability Scanning

**System and Services Acquisition**
System and Services Acquisition Policy and Procedures, Allocation of Resources, Life Cycle Support, Acquisitions, Information System Documentation, Software Usage Restrictions, User Installed Software, Security Design Principles, Outsourced Information System Services, Developer Configuration Management, Developer Security Testing

**System and Communications Protection**
System and Communications Protection Policy and Procedures, Application Partitioning, Security Function Isolation, Information Remnants, Denial of Service Protection, Resource Priority, Boundary Protection, Transmission Integrity, Transmission Confidentiality, Network Disconnect, Trusted Path, Cryptographic Key Establishment and Management, Use of Validated Cryptography, Public Access Protections, Collaborative Computing, Transmission of Security Parameters, Public Key Infrastructure Certificates, Mobile Code, Voice Over Internet Protocol

**System and Information Integrity**
System and Information Integrity Policy and Procedures, Flaw Remediation, Malicious Code Protection, Intrusion Detection Tools and Techniques, Security Alerts and Advisories, Security Functionality Verification, Software and Information Integrity, Spam and Spyware Protection, Information Input Restrictions, Information Input Accuracy, Completeness, and Validity, Error Handling, Information Output Handling and Retention

[NIST06] suggests that adjustments may be needed for considerations related to the following:

- **Technology:** Some controls are only applicable to specific technologies, and hence these controls are only needed if the system includes those technologies. Examples of these include wireless networks and the use of cryptography. Some may only be appropriate if the system supports the technology they require; for example, readers for access tokens. If these technologies are not supported on a system, then alternate controls, including administrative procedures or physical access controls, may be used instead.
- **Common controls:** The entire organization may be managed centrally and may not be the responsibility of the managers of a specific system. Control changes would need to be agreed to and managed centrally.
- **Public access systems:** Some systems, such as the organization's public Web server, are designed to be accessed by the general public. Some controls, such as those relating to personnel security, identification, and authentication, would not apply to access via the public interface. They would apply to administrative control of such systems. The scope of application of such controls must be specified carefully.
- **Infrastructure controls:** Physical access or environmental controls are only relevant to areas housing the relevant equipment.
- **Scalability issues:** Controls may vary in size and complexity in relation to the organization employing them. For example, a contingency plan for systems critical to a large organization would be much larger and more detailed than that for a small business.
- **Risk assessment:** Controls may be adjusted according to the results of specific risk assessment of systems in the organization, as we now consider.

If some form of informal or formal risk assessment process is being used, then it provides guidance on specific risks to an organization's IT systems that need to be addressed. These will typically be some selection of operational or technical controls that together can reduce the likelihood of the identified risk occurring, the consequences if it does, or both, to an acceptable level. These may be in addition to those controls already selected in the baseline, or may simply be more detailed and careful specification and use of already selected controls.

The process illustrated in Figure 17.1 indicates that a recommended list of controls should be made to address each risk needing treatment. The recommended controls need to be compatible with the organization's systems and policies, and their selection may also be guided by legal requirements. The resulting list of controls should include details of the feasibility and effectiveness of each control. The feasibility addresses factors such as technical compatibility with and operational impact on existing systems and users' likely acceptance of the control. The effectiveness equates the cost of implementation against the reduction in level of risk achieved by implementing the control.

The reduction in level of risk that results from implementing a new or enhanced control results from the reduction in threat likelihood or consequence that the control provides, as shown in Figure 17.3 (reproduced from Fig 4-4 in [NIST02]).

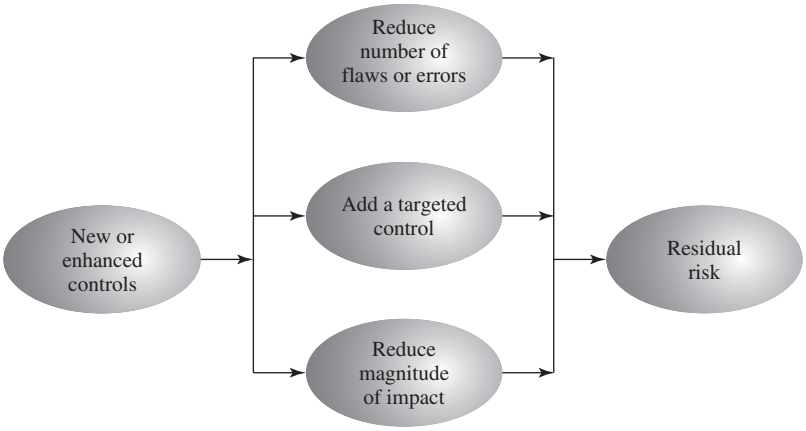


**Figure 17.3** **Residual Risk**

The reduction in likelihood may result either by reducing the vulnerabilities (flaws or weaknesses) in the system or by reducing the capability and motivation of the threat source. The reduction in consequence occurs by reducing the magnitude of the adverse impact of the threat occurring in the organization.

It is likely that the organization will not have the resources to implement all the recommended controls. Therefore, management should conduct a cost/benefit analysis to identify which controls are most appropriate and provide the greatest benefit to the organization given the available resources. This analysis may be qualitative or quantitative and must demonstrate that the cost of implementing a given control is justified by the reduction in level of risk to assets that it provides. It should include details of the impact of implementing the new or enhanced control, the impact of not implementing it, and the estimated costs of implementation. It must then assess the implementation costs and benefits against system and data criticality to determine the importance of choosing this control.

Management must then determine which selection of controls provides an acceptable resulting level of risk to the organization's systems. This selection will consider factors such as the following:

- If the control would reduce risk more than needed, then a less expensive alternative could be used.
- If the control would cost more than the risk reduction provided, then an alternative should be used.
- If a control does not reduce the risk sufficiently, then either more or different controls should be used.
- If the control provides sufficient risk reduction and is the most cost effective, then use it.

It is often the case that the cost of implementing a control is more tangible and easily specified than the cost of not implementing it. Management must make a business decision regarding these ill-defined costs in choosing the final selection of controls and resulting residual risk.

## 17.3 IT SECURITY PLAN

Having identified a range of possible controls from which management has selected some to implement, an IT security plan should then be created. This is a document that provides details as to what will done, what resources are needed, and who will be responsible. The goal is to detail the actions needed to improve the identified deficiencies in the organization's risk profile in a timely manner. [NIST02] suggests that this plan should include details of

- Risks (asset/threat/vulnerability combinations)
- Recommended controls (from the risk assessment)
- Action priority for each risk
- Selected controls (on the basis of the cost/benefit analysis)
- Required resources for implementing the selected controls
- Responsible personnel
- Target start and end dates for implementation
- Maintenance requirements and other comments

These details are summarized in an implementation plan table, such as that shown in Table 17.4. This illustrates an example implementation plan for the example risk identified and shown in Table 16.5. The suggested controls are specific examples of remote access, auditable event, user identification, system backup, and configuration change controls, applied to the identified threatened asset. All of them are chosen, because they are neither costly nor difficult to implement. They do require some changes to procedures. The relevant network administration

**Table 17.4** Implementation Plan

| Risk (Asset/ Threat) | Level of Risk | Recommended Controls | Priority | Selected Controls | Required Resources | Responsible Persons | Start—End Date | Other Comments |
|---|---|---|---|---|---|---|---|---|
| Hacker attack on Internet router | High | • Disable external telnet access<br>• Use detailed auditing of privileged command use<br>• Set policy for strong admin passwords<br>• Set backup strategy for router configuration file<br>• Set change control policy for the router configuration | High | • Strengthen access authentication<br>• Install intrusion detection software | • 3 days IT net admin time to change & verify router configuration, write policies;<br>• 1 day of training for network administration staff | John Doe, Lead Network System Administrator, Corporate IT Support Team | 1-Feb-2006 to 4-Feb-2006 | • Need periodic test and review of configuration and policy use |

staff must be notified of these changes. Staff members may also require training on the correct implementation of the new procedures, and their rights and responsibilities.

## 17.4 IMPLEMENTATION OF CONTROLS

The next phase in the IT security management process is to manage the implementation of the controls detailed in the IT security plan. This comprises the *do* stage of the cyclic implementation model discussed in Section 16.1. The implementation phase comprises not only the direct implementation of the controls as detailed in the security plan, but also the associated specific training and general security awareness programs for the organization.

### Implementation of Security Plan

The IT security plan documents what needs to be done for each selected control, along with the personnel responsible, and the resources and time frame to be used. The identified personnel then undertake the tasks needed to implement the new or enhanced controls, be they technical, managerial, or operational. This may involve some combination of system configuration changes, upgrades, or new system installation. It may also involve the development of new or extended procedures to document practices needed to achieve the desired security goals. Note that even technical controls typically require associated operational procedures to ensure their correct use. The use of these procedures needs to be encouraged and monitored by management.

The implementation process should be monitored to ensure its correctness. Usually this is done by the organizational security officer, who checks that

- The implementation costs and resources used stay within identified bounds.
- The controls are correctly implemented as specified in the plan, in order that the identified reduction in risk level is achieved.
- The controls are operated and administered as needed.

When the implementation is successfully completed, management needs to authorize the system for operational use. This may be a purely informal process within the organization. Alternatively, especially in government organizations, this may be part of a formal process resulting in accreditation of the system as meeting required standards. This is usually associated with the installation, certification, and use of trusted computing system, as we discuss in Chapter 10. In these cases an external accrediting body will verify the documented evidence of the correct design and implementation of the system.

### Security Training

Appropriate security training is an essential component in implementing controls. This training is targeted at the personnel responsible for the development, operation, and administration of the system being installed or enhanced. This training

may involve details of the design and implementation of technical controls, particularly if these are new or changed significantly from those controls used previously in the organization. It may also involve awareness of details in operational procedures associated with the system, to ensure their correct use.

### Security Awareness

In addition to specific training relating to particular systems and controls, there is usually a need for general security awareness training for all personnel in an organization. Such awareness is essential for most organizations to meet their security objectives. Experience shows that a lack of security awareness and associated poor security practices by personnel can significantly reduce the effectiveness of security controls. It has long been recognized that people are often the weakest link in managing security in an organization. The aim of a security awareness program is to convince personnel that significant risks exist to the organization's IT infrastructure and that a security breach could have major consequences for the organization.

The security awareness program should address issues such as

- The organization's security objectives, strategies, and policies
- The need for security and the general risks the organization is exposed to
- Understanding of why security controls, including technical measures and operational procedures, are used
- The roles and responsibilities for various groups of personnel
- The need to act in accordance with policy and procedures, and the consequences of unauthorized actions
- The need to report any security breaches observed and to assist with their investigation

This program should span all levels in the organization, from senior management down. Larger organizations would usually have a range of programs targeted at the various levels, addressing their needs and requirements appropriately.

A wide range of activities and material can be used in such a program. This can include publicity material such as posters, memos, newsletters, and flyers that detail key aspects of security policies and act to generally raise awareness of the issues from day to day. It can also include various workshops and training sessions for groups of staff, providing information relevant to their needs. These may often be incorporated into more general training programs on organizational practices and systems. The standards encourage the use of examples of good practice that are related to the organization's systems and IT usage. The more relevant and easy to follow the procedures are, the more likely it is that a greater level of compliance and hence security will be achieved.

Suitable security awareness sessions should be incorporated into the process used to introduce new staff to the organization and its processes. Security awareness sessions should also be repeated regularly to help staff members refresh their knowledge and understanding of security issues.

## 17.5 IMPLEMENTATION FOLLOW-UP

The IT security management process does not end with the implementation of controls and the training of personnel. As we noted in Chapter 16, it is a cyclic process, constantly repeated to respond to changes in the IT systems and the risk environment. The various controls implemented should be monitored to ensure their continued effectiveness. Any proposed changes to systems should be checked for security implications and the risk profile of the affected system reviewed if necessary. Unfortunately, this aspect of IT security management often receives the least attention and in many cases is added as an afterthought, if at all. Failure to do so can greatly increase the likelihood that a security failure will occur. This follow-up stage of the management process includes a number of aspects:

- Maintenance of security controls
- Security compliance checking
- Change and configuration management
- Incident handling

Any of these aspects might indicate that changes are needed to the previous stages in the IT security management process. An obvious example is that should a breach occur, such as a virus infection of desktop systems, then changes may be needed to the risk assessment, to the controls chosen, or to the details of their implementation. This can trigger a review of earlier stages in the process.

### Maintenance

The first aspect concerns the continued maintenance and monitoring of the implemented controls, to ensure their continued correct functioning and appropriateness. It is important that someone has responsibility for this maintenance process, which is generally coordinated by the organization's security officer. The maintenance tasks include ensuring that

- Controls are periodically reviewed to verify that they still function as intended.
- Controls are upgraded when new requirements are discovered.
- Changes to systems do not adversely affect the controls.
- New threats or vulnerabilities have not become known.

The goal of maintenance is to ensure that the controls continue to perform as intended, and hence that the organization's risk exposure remains as chosen. Failure to maintain controls could lead to a security breach with a potentially significant impact on the organization.

### Security Compliance

Security compliance checking is an audit process to review the organization's security processes. The goal is to verify compliance with the security plan. The audit may be conducted using either internal or external personnel. It is generally based on

the use of checklists, which verify that the suitable policies and plans have been created, that suitable controls were chosen, and that the controls are maintained and used correctly.

This audit process may be performed as part of a wider, general audit of the organization's management.

### Change and Configuration Management

Change management is the process used to review proposed changes to systems for implications on the organization's systems and use. Changes to existing systems can occur for a number of reasons, such as the following:

- Users reporting problems or desired enhancements
- Identification of new threats or vulnerabilities
- Vendor notification of patches or upgrades to hardware or software
- Technology advances
- Implementation of new IT features or services, which require changing existing systems
- Identification of new tasks, which require changing existing systems

The impact of any proposed change on the organization's systems should be evaluated. This includes not only security-related aspects, but wider operational issues as well. Thus change management is an important component of the general systems administration process. Because changes can affect security, this general process overlaps IT security management, and must interact with it.

An important example is the constant flow of patches addressing bugs and security failings in common operating systems and applications. If the organization is running systems of any complexity, with a range of applications, then patches should ideally be tested to ensure that they don't adversely affect other applications. This can be a time-consuming process that may require considerable administration resources. If patch testing is not done, one alternative is to delay patching or upgrading systems. This could leave the organization exposed to a new vulnerability for a period. Otherwise the patches or upgrades could be applied without testing, which may result in other failures in the systems and the loss of functionality.

Ideally, most proposed changes should act to improve the security profile of a system. However, it is possible that for imperative business reasons a change is proposed that reduces the security of a system. In cases like this, it is important that the reasons for the change, its consequences on the security profile for the organization, and management authorization of it be documented. The benefits to the organization would need to be traded off against the increased risk level.

The change management process may be informal or formal, depending on the size of the organization and its overall IT management processes. In a formal process, any proposed change should be documented and tested before implementation. As part of this process, any related documentation, including relevant security documentation and procedures, should be updated to reflect the change.

Configuration management is concerned with specifically keeping track of the configuration of each system in use and the changes made to each. This includes lists

of the hardware and software versions installed on each system. This information is needed to help restore systems following a failure (whether security related or not) and to know what patches or upgrades might be relevant to particular systems. Again, this is a general systems administration process with security implications and must interact with IT security management.

### Incident Handling

The procedures used to respond to a security incident comprise the final aspect included in the follow-up stage of IT security management. The development of such procedures is regarded as an essential control for most organizations. Most organizations will experience some form of security incident sooner rather than later. Typically most incidents relate to risks with lesser impacts on the organization, but occasionally a more serious incident can occur. The incident response procedures need to reflect the range of possible consequences of an incident on the organization and allow for a suitable response. By developing suitable procedures in advance, an organization can avoid the panic that occurs when personnel realize that bad things are happening and are not sure of the best response. More formally, [NIST04] lists the following benefits of having an incident response capability:

- Responding to incidents systematically so that the appropriate steps are taken
- Helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services
- Using information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data
- Dealing properly with legal issues that may arise during incidents

Consider the example of a mass e-mail worm infection of an organization. There have been numerous examples of these in recent years. They typically exploit unpatched vulnerabilities in common desktop applications and then spread via e-mail to other addresses known to the infected system. The volume of traffic these can generate could be high enough to cripple both intranet and Internet connections. Faced with such an impact, an obvious response is to disconnect the organization from the wider Internet, and perhaps to shut down the internal e-mail system. This decision could, however, have a serious impact on the organization's processes, which must be traded off against the reduced spread of infection. At the time the incident is detected, the personnel directly involved may not have the information to make such a critical decision about the organization's operations. A good incident response policy should indicate the action to take for an incident of this severity. It should also specify the personnel who have the responsibility to make decisions concerning such significant actions and detail how they can be quickly contacted to make such decisions.

There is a range of events that can be regarded as a security incident. Indeed any action that threatens one or more of the classic security services of confidentiality, integrity, availability, accountability, authenticity, and reliability in a system constitutes

an incident. These include various forms of unauthorized access to a system and unauthorized modification of information on the system. Unauthorized access to a system by a person includes

- Accessing information that person is not authorized to see
- Accessing information and passing it on to another person who is not authorized to see it
- Attempting to circumvent the access mechanisms implemented on a system
- Using another person's password and user id for any purpose
- Attempting to deny use of the system to any other person without authorization to do so

Unauthorized modification of information on a system by a person includes

- Attempting to corrupt information that may be of value to another person
- Attempting to modify information and/or resources without authority
- Processing information in an unauthorized manner

Managing security incidents involves procedures and controls that address

- Detecting potential security incidents
- Identifying and responding to breaches in security
- Documenting breaches in security for future reference

This process is illustrated in Figure 17.4, adapted from figure 3-1 in [NIST04]. Information learned as a result of a security incident should be used to improve procedures and the risk profile in the future.

**Detecting Incidents** Security incidents may be detected by users or administration staff, who report a system malfunction or anomalous behavior. Staff should be encouraged to make such reports. Staff should also report any suspected weaknesses in systems. The general security training of staff in the organization should include details of who to contact in such cases.

Security incidents may also be detected by automated tools, which analyze information gathered from the systems and connecting networks. We discuss a range of such tools in Chapter 6. These tools may report evidence of either a precursor to a possible future incident or indication of an actual incident occurring. Tools that can detect incidents include the following:

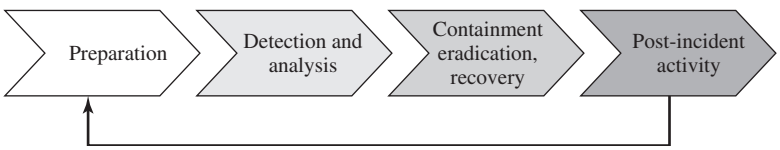


**Figure 17.4 Incident Response Life Cycle**

- **System integrity verification tools:** Scan critical system files, directories, and services to ensure they have not been changed without proper authorization.
- **Log analysis tools:** Analyze the information collected in audit logs using some form of pattern recognition to identify potential security incidents.
- **Network and host intrusion detection systems:** Monitor and analyze network and host activity and usually compare this information with a collection of attack signatures to identify potential security incidents.
- **Intrusion prevention systems:** Augment an intrusion detection system with the ability to automatically block detected attacks. Such systems need to be used with care, because they can cause problems if they respond to a misidentified attack and reduce system functionality when not justified. We discuss such systems in Section 9.6.

The effectiveness of such automated tools depends greatly on the accuracy of their configuration, and the correctness of the patterns and signatures used. The tools need to be updated regularly to reflect new attacks or vulnerabilities. They also need to distinguish adequately among normal, legitimate behavior, and anomalous attack behavior. This is not always easy to achieve and depends on the work patterns of specific organizations and their systems. However, a key advantage of automated systems that are regularly updated is that they can track changes in known attacks and vulnerabilities. It is often difficult for security administrators to keep pace with the rapid changes to the security risks to their systems and to respond with patches or other changes needed in a timely manner. The use of automated tools can help reduce the risks to the organization from this delayed response.

The decision to deploy automated tools should result from the organization's security goals and objectives and specific needs identified in the risk assessment process. Deploying these tools usually involves significant resources, both monetary and in personal time. This needs to be justified by the benefits gained in reducing risks.

Whether or not automated tools are used, the security administrators need to monitor reports of vulnerabilities and to respond with changes to their systems if necessary.

**Responding to Incidents** Once a potential incident is detected, there must be documented procedures to respond to it. These procedures must detail how to identify the cause of the security incident, whether accidental or deliberate. The procedures then must describe the action taken to recover from the incident in a manner that minimizes the compromise or harm to the organization. It is clearly impossible to detail every possible type of incident. However, the procedures should identify typical categories of such incidents and the approach taken to respond to them. Ideally these should include descriptions of possible incidents and typical responses. They should also identify the management personnel responsible for making critical decisions affecting the organization's systems and how to contact them at any time when an incident is occurring. This is particularly important in circumstances such as the mass e-mail worm infection we described, when the response involves trading off major loss of functionality against further significant systems compromise. Such decisions will clearly affect the organi-

zation's operations and must be made very quickly. [NIST04] lists the following broad categories of security incidents that should be addressed in incident response policies:

- Denial-of-service attacks that prevent or impair normal use of systems
- Malicious code that infects a host
- Unauthorized access to a system
- Inappropriate usage of a system in violation of acceptable use policies
- Multiple-component incidents, which involve two or more of the above categories in a single incident

In determining the appropriate responses to an incident, a number of issues should be considered. These include how critical the system is to the organization's function and the current and potential technical effect of the incident in terms of how significantly the system has been compromised.

The response procedures should also identify the circumstances when security breaches should be reported to third parties such as the police or relevant CERT organization. There is a high degree of variance among organizational attitudes to such reports. Making such reports clearly helps third parties monitor the overall level of activity and trends in computer crimes. However, particularly if legal action could be instituted, it may be a liability for the organization to gather and present suitable evidence. While the law may require reporting in some circumstances, there are many other types of security incidents when the response is not prescribed. Hence it must be determined in advance when such reports would be regarded as appropriate for the organization. There is also a chance that if an incident is reported externally, it might be reported in the public media. An organization should identify how it would respond in general to such reports.

For example, an organization could decide that cases of computer-assisted fraud should be reported to both the police and the relevant CERT, with the aim of prosecuting the culprit and recovering any losses. Breaches of personal information are often now required by law to be reported to the relevant authorities and suitable responses taken. However, an incident such as a Web site defacement is unlikely to lead to a successful prosecution. Hence the policy might be for the organization to report these incidents to the relevant CERT and to take steps in response to restore functionality as quickly as possible and to minimize the possibility of a repeat attack.

As part of the response to an incident, evidence is gathered about the incident. Initially this information is used to help recover from the incident. If the incident is reported to the police, then this evidence may also be needed for legal proceedings. In this case, it is important that careful steps are taken to document the collection process for the evidence and its subsequent storage and transfer. If this is not done in accordance with the relevant legal procedures, it is likely the evidence will not be admissible in court. The procedures required vary from country to country. [NIST04] includes some guidance on this issue.

**Documenting Incidents** Following the immediate response to an incident, there is a need to identify what vulnerability led to its occurrence and how this might be addressed to prevent the incident in the future. Details of the incident

and the response taken are recorded for future reference. The impact on the organization's systems and their risk profile must also be reconsidered as a result of the incident.

This typically involves feeding the information gathered as a result of the incident back to an earlier phase of the IT security management process. It is possible that the incident was an isolated rare occurrence and the organization was simply unlucky for it to occur. More generally, though, a security incident reflects a change in the risk profile of the organization that needs to be addressed. This could involve reviewing the risk assessment of the relevant systems and either changing or extending this analysis. It could involve reviewing controls identified for some risks, strengthening existing controls, and implementing new controls. This reflects the cyclic process of IT security management.

## 17.6 CASE STUDY: SILVER STAR MINES

Consider the case study introduced in Chapter 16, which involves the operations of a fictional company, Silver Star Mines. Given the outcome of the risk assessment for this company, the next stage in the security management process is to identify possible controls. From the information provided during this assessment, clearly a number of the possible controls listed in Table 17.3 are not being used. A comment repeated many times was that many of the systems in use had not been regularly upgraded, and part of the reason for the identified risks was the potential for system compromise using a known but unpatched vulnerability. That clearly suggests that attention needs to be given to controls relating to the regular, systematic maintenance of operating systems and applications software on server and client systems. Such controls include

- Configuration management policy and procedures
- Baseline configuration
- System maintenance policy and procedures
- Periodic maintenance
- Flaw remediation
- Malicious code protection
- Spam and spyware protection

Given that potential incidents are possible, attention should also be given to developing contingency plans to detect and respond to such incidents and to enable speedy restoration of system function. Attention should be paid to controls such as

- Audit monitoring, analysis, and reporting
- Audit reduction and report generation
- Contingency planning policy and procedures
- Incident response policy and procedures
- Information system backup
- Information system recovery and reconstitution

These controls are generally applicable to all the identified risks and constitute good general systems administration practice. Hence their cost-effectiveness would be high because they provide an improved level of security across multiple identified risks.

Now consider the specific risk items. The top-priority risk relates to the reliability and integrity of the Supervisory Control and Data Acquisition (SCADA) nodes and network. These were identified as being at risk because many of these systems are running older releases of operating systems with known insecurities. Further, these systems cannot be patched or upgraded because the key applications they run have not been updated or validated to run on newer O/S versions. Given these limitations on the ability to reduce the vulnerability of individual nodes, attention should be paid to the firewall and application proxy servers that isolate the SCADA nodes and network from the wider corporate network. These systems can be regularly maintained and managed according to the generally applied list of controls we identified. Further, because the traffic to and from the SCADA network is highly structured and predictable, it should be possible to implement an intrusion detection system with much greater reliability than applies to general-use corporate networks. This system should be able to identify attack traffic, as it would be very different from normal traffic flows. Such a system might involve a more detailed, automated analysis of the audit records generated on the existing firewall and proxy server systems. More likely it could be an independent system connected to and monitoring the traffic through these systems. The system could be further extended to include an automated response capability, which could automatically sever the network connection if an attack is identified. This approach recognizes that the network connection is not needed for the correct operation of the SCADA nodes. Indeed, they were designed to operate without such a network connection, which is much of the reason for their insecurity. All that would be lost is the improved overall monitoring and management of the SCADA nodes. With this functionality, the likelihood of a successful attack, already regarded as very unlikely, can be further reduced.

The second priority risk relates to the integrity of stored information. Clearly all the general controls help ameliorate this risk. More specifically, much of the problem relates to the large number of documents scattered over a large number of systems with inconsistent management. This risk would be easier to manage if all documents identified as critical to the operation of the company were stored on a smaller pool of application and file servers. These could be managed appropriately using the generally applicable controls. This suggests that an audit of critical documents is needed to identify who is responsible for them and where they are currently located. Then policies are needed that specify that critical documents should be created and stored only on approved central servers. Existing documents should be transferred to these servers. Appropriate education and training of all affected users is needed to help ensure that these policies are followed.

The next three risks relate to the availability or integrity of the key financial, procurement, and maintenance/production systems. The generally applicable controls we identified should adequately address these risks once the controls are applied to all relevant servers.

The final risk relates to the availability, integrity, and confidentiality of e-mail. As was noted in the risk assessment, this is primarily the responsibility of the parent com-

**Table 17.5** Silver Star Mines—Implementation Plan

| Risk (Asset/Threat) | Level of Risk | Recommended Controls | Priority | Selected Controls |
|---|---|---|---|---|
| All risks (generally applicable) | | 1. Configuration and periodic maintenance policy for servers<br>2. Malicious code (SPAM spyware) prevention<br>3. Audit monitoring, analysis, reduction, and reporting on servers<br>4. Contingency planning and incident response policies and procedures<br>5. System backup and recovery procedures | 1 | 1.<br>2.<br>3.<br>4.<br>5. |
| Reliability and integrity of SCADA nodes and network | High | 1. Intrusion detection and response system | 2 | 1. |
| Integrity of stored file and database information | Extreme | 1. Audit of critical documents<br>2. Document creation and storage policy<br>3. User security education and training | 3 | 1.<br>2.<br>3. |
| Availability and integrity of financial, procurement, and maintenance/production systems | High | — | — | (general controls) |
| Availability, integrity, and confidentiality of e-mail | High | 1. Contingency planning—backup e-mail service | 4 | 1. |

pany's IT group that manages the external mail gateway. There is a limited amount that can be done on the local site. The use of the generally applicable controls, particularly those relating to malicious code protection and spam and spyware protection on client systems, will assist in reducing this risk. In addition, as part of the contingency planning and incident response policies and procedures, consideration could be given to a backup e-mail system. For security this system would use client systems isolated from the company intranet, connected to an external local network service provider. This connection would be used to provide limited e-mail capabilities for critical messages should the main company intranet e-mail system be compromised.

This analysis of possible controls is summarized in Table 17.5, which lists the controls identified and the priorities for their implementation. This table must be extended to include details of the resources required, responsible personnel, time frame, and any other comments. This plan would then be implemented, with suitable monitoring of its progress. Its successful implementation leads then to longer term follow-up, which ensures that the new policies continue to be applied appropriately and that regular reviews of the companies security profile occur. In time this should lead to a new cycle of risk assessment, plan development, and follow-up.

## 17.7 RECOMMENDED READING

More general discussion of the issues involved with IT security management is found in [MAIW02] and [SLAY06]. Current best practice in the field of IT security management is codified in a range of international and national standards, whose use is encouraged. These standards include [ISO13335], [ISO17799], [ISO27001], [NIST95], [NIST02], [NIST04], [NIST05], and [NIST06].

**ISO13335** ISO/IEC, "ISO/IEC 13335–1:2004—Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management." Part 2 on operational guidance for ICT security management will be released soon.

**ISO17799** ISO/IEC, "ISO/IEC 17799:2005—Information technology—Security techniques—Code of practice for information security management." Will be replaced by ISO27002.

**ISO27001** ISO/IEC, "ISO/IEC 27001:2005—Information technology—Security Techniques—Information security management systems—Requirements." This replaces the older Australian and British national standards AS7799.2 and BS7799.2.

**MAIW02** Maiwald, E., and Sieglein, W. *Security Planning & Disaster Recovery*, Berkeley, CA: McGraw-Hill/Osborne, 2002.

**NIST95** National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800–12. October 1995.

**NIST02** National Institute of Standards and Technology. *Risk Management Guide for Information Technology Systems*. Special Publication 800–30. July 2002.

**NIST04** National Institute of Standards and Technology. *Computer Security Incident Handling Guide*. Special Publication 800–61. January 2004.

**NIST05** National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems.* Special Publication 800–53. February 2005.

**NIST06** National Institute of Standards and Technology. *Guide for Developing Security Plans for Federal Information Systems*. Special Publication 800–18 Revision 1. February 2006.

**SLAY06** Slay, J., and Koronios, A. *Information Technology Security & Risk Management*, Milton, Qld: John Wiley & Sons Australia, 2006.

## 17.8 KEY TERMS, REVIEW QUESTIONS, AND PROBLEMS

### Key Terms

| | | |
|---|---|---|
| change management | implementation plan | safeguard |
| configuration management | incident handling | security compliance |
| control | IT security plan | security training |
| detection and recovery control | management control | supportive control |
| | operational control | technical control |
| | preventative control | |

## Review Questions

17.1 Define *security control* and *safeguard*.

17.2 List and briefly define the three broad classes of controls and the three categories each can include.

17.3 List a specific example of each of three broad classes of controls from those given in Table 17.3.

17.4 List the steps [NIST02] specifies for selecting and implementing controls.

17.5 List three ways that implementing a new or enhanced control can reduce the residual level of risk.

17.6 List the items that should be included in an IT security implementation plan.

17.7 List and briefly define the elements from the implementation of controls phase of IT security management.

17.8 List and briefly define the elements from the implementation follow-up phase of IT security management.

17.9 What are the benefits of developing an incident response capability?

17.10 List the broad categories of security incidents.

17.11 List some types of tools used to detect and respond to incidents.

17.12 What should occur following the handling of an incident with regard to the overall IT security management process?

## Problems

17.1 Consider the risk to "integrity of customer and financial data files on system" from "corruption of these files due to import of a worm/virus onto system," as discussed in Problem 16.2. From the list shown in Table 17.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost-effective.

17.2 Consider the risk to "integrity of the accounting records on the server" from "financial fraud by an employee, disguised by altering the accounting records," as discussed in Problem 16.3. From the list shown in Table 17.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost-effective.

17.3 Consider the risk to "integrity of the organization's Web server" from "hacking and defacement of the Web server," as discussed in Problem 16.4. From the list shown in Table 17.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost-effective.

17.4 Consider the risk to "confidentiality of techniques for conducting penetration tests on customers, and the results of these tests, which are stored on the server" from "theft/breach of this confidential and sensitive information," as discussed in Problem 16.5. From the list shown in Table 17.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost-effective.

17.5 Consider the risk to "confidentiality of personnel information in a copy of a database stored unencrypted on the laptop" from "theft of personal information, and its subsequent use in identity theft caused by the theft of the laptop," as discussed in Problem 16.6. From the list shown in Table 17.3, select some suitable specific controls that could reduce this risk. Indicate which you believe would be most cost-effective.

17.6 Consider the risks you determined in the assessment of a small public service agency, as discussed in Problem 18.7. Select what you believe are the most critical risks, and suggest some suitable specific controls from the list shown in Table 17.3 that could reduce these risks. Indicate which you believe would be the most cost-effective.

**17.7** Consider the development of an incident response policy for the small accounting firm mentioned in Problems 16.2 and 17.1. Specifically consider the response to the detection of an e-mail worm infecting some of the company systems and producing large volumes of e-mail spreading the propagation. What default decision do you recommend the firm's incident response policy dictate regarding disconnecting the firm's systems from the Internet to limit further spread? Take into account the role of such communications on the firm's operations. What default decision do you recommend regarding reporting this incident to the appropriate computer emergency response team (CERT)? Or to the relevant law enforcement authorities?

**17.8** Consider the development of an incident response policy for the small legal firm mentioned in Problems 16.3 and 17.2. Specifically consider the response to the detection of financial fraud by an employee. What initial actions should the incident response policy specify? What default decision do you recommend regarding reporting this incident to the appropriate CERT? Or to the relevant law enforcement authorities?

**17.9** Consider the development of an incident response policy for the Web design company mentioned in Problems 16.4 and 17.3. Specifically consider the response to the detection of hacking and defacement of the company's Web server. What default decision do you recommend the company's incident response policy dictate regarding disconnecting this system from the Internet to limit damaging publicity? Take into account the role of this server in promoting the company's operations. What default decision do you recommend regarding reporting this incident to the appropriate CERT? Or to the relevant law enforcement authorities?

**17.10** Consider the development of an incident response policy for the large government department mentioned in Problems 16.6 and 17.5. Specifically consider the response to the report of theft of an officially issued laptop from a department employee, which is subsequently found to have contained a large number of sensitive personnel records. What default decision do you recommend the department's incident response policy dictate regarding contacting the personnel whose records have been stolen? What default decision should be taken regarding sanctioning the employee whose laptop was stolen? Take into account any relevant legal requirements and sanctions that may apply, and the necessity for relevant items in the department's IT policy regarding actions. What default decision do you recommend regarding reporting this incident to the appropriate CERT? Or to the relevant law enforcement authorities?