CHAPTER 14

Human Factors

The subject of human factors as it relates to computer security is a broad one, and a full discussion is well beyond the scope of this book. In this chapter, we touch on a few important topics in this area.

14.1 SECURITY AWARENESS, TRAINING, AND EDUCATION

The topic of security awareness, training, and education is mentioned prominently in a number of standards and standards-related documents, including ISO 17799 (*Code of Practice for Information Security Management*) and NIST Special Publication 800-100 (*Information Security Handbook: A Guide for Managers*). This section provides an overview of the topic.

Motivation

Security awareness, training, and education programs provide four major benefits to organizations:

- Improving employee behavior
- Increasing the ability to hold employees accountable for their actions
- Mitigating liability of the organization for an employee's behavior
- Complying with regulations and contractual obligations

Employee behavior is a critical concern in ensuring the security of computer systems and information assets. Employee actions account for more computer-related loss and security compromises than all other sources combined [NIST95]. The principal problems associated with employee behavior are errors and omissions, fraud, and actions by disgruntled employees. Security awareness, training, and education programs can reduce the problem of errors and omissions.

Such programs can serve as a deterrent to fraud and actions by disgruntled employees by increasing employees' knowledge of their **accountability** and of potential penalties. Employees cannot be expected to follow policies and procedures of which they are unaware. Further, enforcement is more difficult if employees can claim ignorance when caught in a violation.

Ongoing security awareness, training, and education programs are also important in limiting an organization's **liability**. Such programs can bolster an organization's claim that a standard of due care has been taken in protecting information.

Finally, security awareness, training, and education programs may be needed to comply with **regulations and contractual obligations**. For example, companies that have access to information from clients may have specific awareness and training obligations that they must meet for all employees with access to client data.

A Learning Continuum

A number of NIST documents, as well as ISO 17799, recognize that the learning objectives for an employee with respect to security depend on the employee's role. There is a need for a continuum of learning programs that starts with awareness, builds to training, and evolves into education. Figure 14.1 shows a model that outlines the learning needed as an employee assumes different roles and responsibilities with respect to information systems, including equipment and data. Beginning at the bottom of the model, all employees need an awareness of the importance of security and a general understanding of policies, procedures, and restrictions. Training, represented by the two middle layers, is required for individuals who will be using IT systems and data and therefore need more detailed knowledge of IT security threats, vulnerabilities, and safeguards. The top layer applies primarily to individuals who have a specific role centered on IT systems, such as programmers and those involved in maintaining and managing IS assets and those involved in IS security.

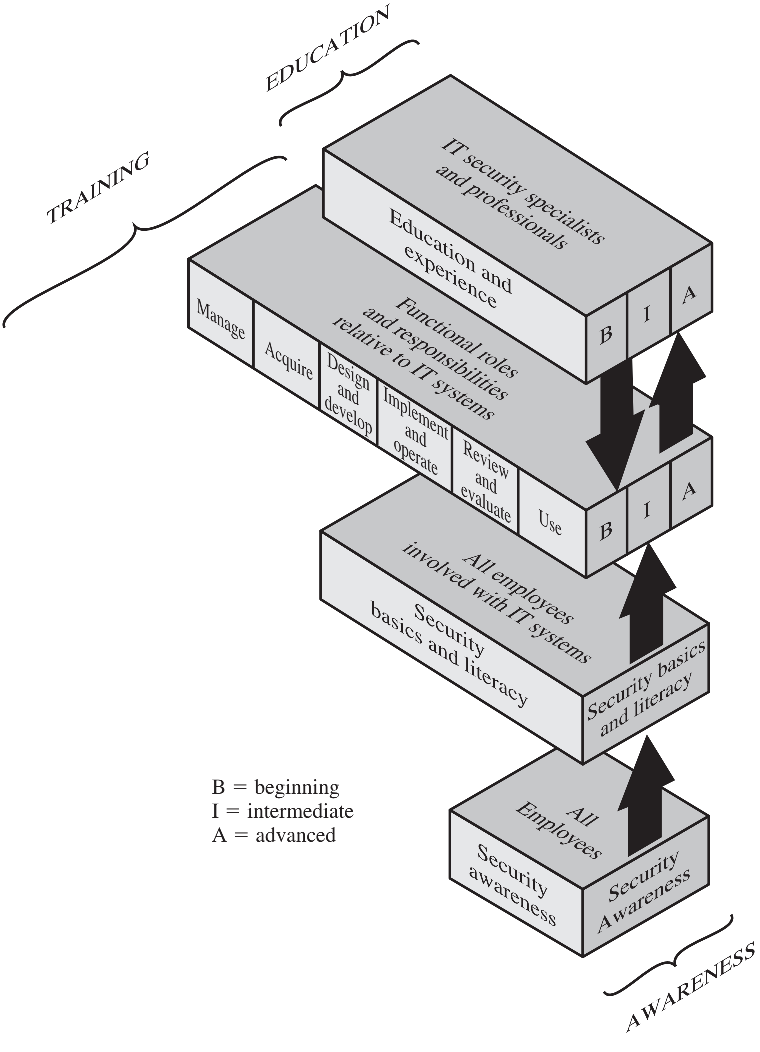

Figure 14.1 **Information Technology (IT) Learning Continuum**

NIST SP 800-16 (*Information Technology Security Training Requirements: A Role- and Performance-Based Model*) summarizes the four layers as follows:

- **Security Awareness** is explicitly required for all employees, whereas Security Basics and Literacy is required for those employees, including contractor employees, who are involved in any way with IT systems. In today's environment the latter category includes almost all individuals within the organization.
- The **Security Basics and Literacy** category is a transitional stage between Awareness and Training. It provides the foundation for subsequent training by providing a universal baseline of key security terms and concepts.
- After Security Basics and Literacy, training becomes focused on providing the knowledge, skills, and abilities specific to an individual's **Roles and Responsibilities Relative to IT Systems**. At this level, training recognizes the differences among beginning, intermediate, and advanced skill requirements.
- The **Education and Experience** level focuses on developing the ability and vision to perform complex, multidisciplinary activities and the skills needed to further the IT security profession and to keep pace with threat and technology changes.

Table 14.1 illustrates some of the distinctions among awareness, training, and education. We look at each of these categories in turn.

Awareness In general, a security awareness program seeks to inform and focus an employee's attention on issues related to security within the organization. The hoped-for benefits from security awareness include the following:

1. Employees are aware of their responsibilities for maintaining security and the restrictions on their actions in the interests of security and are motivated to act accordingly.
2. Users understand the importance of security for the well-being of the organization.
3. Because there is a constant barrage of new threats, user support, IT staff enthusiasm, and management buy-in are critical and can be promoted by awareness programs.

Table 14.1 Comparative Framework

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

The content of an awareness program must be tailored to the needs of the organization and to the target audience, which includes managers, IT professionals, IS users, and employees with little or no interaction with information systems. NIST SP-800-100 (*Information Security Handbook: A Guide for Managers*) describes the content of awareness programs, in general terms, as follows:

> Awareness tools are used to promote information security and inform users of threats and vulnerabilities that impact their division or department and personal work environment by explaining the **what** but not the **how** of security, and communicating what is and what is not allowed. Awareness not only communicates information security policies and procedures that need to be followed, but also provides the foundation for any sanctions and disciplinary actions imposed for noncompliance. Awareness is used to explain the rules of behavior for using an agency's information systems and information and establishes a level of expectation on the acceptable use of the information and information systems.

An awareness program must continually promote the security message to employees in a variety of ways. Examples include the following:

- Events, such as a security awareness day
- Promotional materials, such as newsletters, posters, memos, and videos
- Briefings (program-specific or system-specific or issue-specific)
- An employee security policy document

[SZUB98] provides a useful list of goals for a security awareness program, as follows:

Goal 1: Raise staff awareness of information technology security issues in general.

Goal 2: Ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security.

Goal 3: Explain organizational security policies and procedures.

Goal 4: Ensure that staff understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.

Goal 5: Train staff to meet the specific security responsibilities of their positions.

Goal 6: Inform staff that security activities will be monitored.

Goal 7: Remind staff that breaches in security carry consequences.

Goal 8: Assure staff that reporting of potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making behavior).

Goal 9: Communicate to staff that the goal of creating a trusted system is achievable.

To cement the importance of security awareness, an organization should have a security awareness policy document that is provided to all employees. The policy should establish three things:

1. Participation in an awareness program is required for every employee. This will include an orientation program for new employees as well as periodic awareness activities.
2. Everyone will be given sufficient time to participate in awareness activities.
3. Responsibility for managing and conducting awareness activates is clearly spelled out.

An excellent, detailed list of considerations for security awareness is provided in *The Standard of Good Practice for Information Security*, from the Information Security Forum [ISF05]. This material is reproduced in Appendix 14A.

Training A security training program is designed to teach people the skills to perform their IS-related tasks more securely. Training teaches **what** people should do and **how** they should do it. Depending on the role of the user, training encompasses a spectrum ranging from basic computer skills to more advanced specialized skills.

For general users, training focuses on good computer security practices, including

- Protecting the physical area and equipment (e.g., locking doors, caring for CD-ROMs and DVDs)
- Protecting passwords (if used) or other authentication data or tokens (e.g., never divulge PINs)
- Reporting security violations or incidents (e.g., whom to call if a virus is suspected)

Programmers, developers, and system maintainers require more specialized or advanced training. This category of employees is critical to establishing and maintaining computer security. However, it is the rare programmer or developer who understands how the software that he or she is building and maintaining can be exploited. Typically, developers don't build security into their applications and may not know how to do so, and they resist criticism from security analysts. The training objectives for this group include the following:

- Develop a security mindset in the developer.
- Show the developer how to build security into development life cycle, using well-defined checkpoints.
- Teach the developer how attackers exploit software and how to resist attack.
- Provide analysts with a toolkit of specific attacks and principles with which to interrogate systems.

Management-level training should teach development managers how to make tradeoffs involving risks, costs, and benefits involving security. The manager needs to understand the development life cycle and the use of security checkpoints and security evaluation techniques.

Executive-level training must explain the difference between software security and network security and, in particular, the pervasiveness of software security issues. Executives need to develop an understanding of security risks and costs. Executives need training on the development of risk management goals, means of measurement, and the need to lead by example in the area of security awareness.

Education The most in-depth program is security education. This is targeted at security professionals and those whose jobs require expertise in security. Security education is normally outside the scope of most organization awareness and training programs. It more properly fits into the category of employee career development programs. Often, this type of education is provided by outside sources such as college courses or specialized training programs.

14.2 ORGANIZATIONAL SECURITY POLICY

RFC 2196 (Site Security Handbook) defines *security policy* as follows:

> A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.

The term *security policy* is also used in other contexts. For example, we discuss security policies in Chapter 10 in the context of formal models for confidentiality and integrity. Security policy may refer to specific security rules for specific systems and be focused on technical matters rather than human factors. In this section, we are concerned with security policy in the sense defined RFC 2196.

Motivation

A written security policy document is fundamental. Security policies define acceptable behavior, expected practices, and responsibilities. Without written policies, users and administrators are left to decide important security-related issues for themselves. Without written policies, an employee is free to assume that a particular task is someone else's responsibility, is free to use "I wasn't told" as a defense for a security violation, and is free to complain that a penalty is unfair because it was not stated beforehand. The policy document also provides valuable support for IT staff and lower-level managers in convincing higher-level managers of the need for a particular expenditure or commitment of resources.

A security policy plays four important roles:

1. It makes clear what is being protected and why.
2. It articulates, in general terms, the security procedures, controls, and standards used in the organization.
3. It clearly states the responsibility for that protection.
4. It provides a basis on which to interpret and resolve any later conflicts that may arise.

To fulfill these roles, the security policy must reflect security decisions made by executive management. Before developing the written security policy for employees, decision makers must

1. Identify sensitive information and critical systems.
2. Incorporate local and national laws, contractual obligations, and relevant ethical standards.
3. Define institutional security goals and objectives.
4. Set a course for accomplishing these goals and objectives.
5. Ensure that necessary mechanisms for accomplishing the goals and objectives are in place.

These considerations can be realized in the form of a security policy life cycle, as illustrated in Figure 14.2 (based on [HAMD06]). Briefly, the main steps are as follows:

- **Risk analysis:** This analysis includes a mission statement, asset evaluation, and threat assessment. Chapter 16 explores this topic.
- **Policy development:** The security policy consists of specific security procedures, controls, and standards. The development of these elements is discussed in Chapters 16 and 17.
- **Policy approval:** For the policy to be effective, it needs approval from not only executive management but also from representatives of key organizational departments and groups. Some form of interdepartmental committee should be involved at this stage.

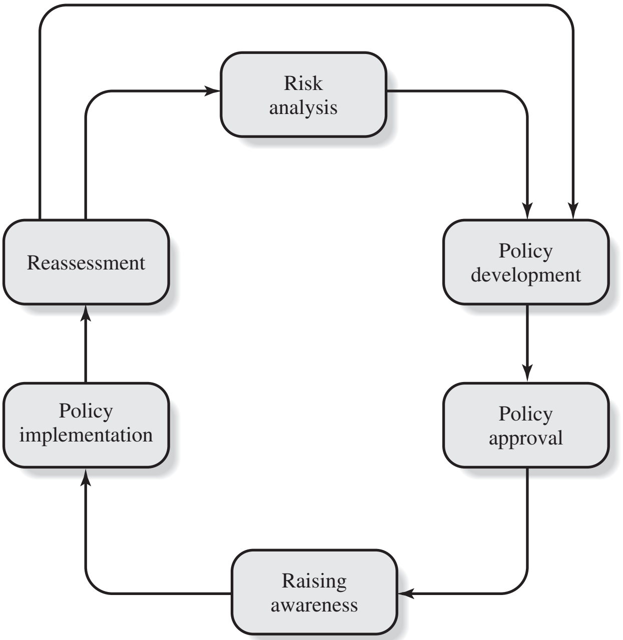

Figure 14.2 **Security Policy Life Cycle**

- **Raising awareness:** We discuss this in Section 14.1.
- **Policy implementation:** Implementation enforces the application of the security policy, using enforcement procedures and mechanisms spelled out in the policy itself.
- **Reassessment:** There needs to be an ongoing, or at least periodic, monitoring and assessment of the various elements of the security policy.

Responsibility for the Security Policy Document

The security policy needs broad support within an organization, at all levels and across all functional areas. The support of top management is essential. Thus a variety of individuals should be involved in formulating policy and generating the security policy document. RFC 2196 suggests the following list of individuals who should be involved in the creation and review of security policy documents:

- Site security administrator
- Information technology technical staff (e.g., staff from computing center)
- Supervisors of large user groups within the organization (e.g., business divisions, computer science department within a university, etc.)
- Security incident response team
- Representatives of the user groups affected by the security policy
- Responsible management
- Legal counsel (if appropriate)

Document Content

The security policy document or documents needs to cover a number of topics, or subject areas, and for each topic provide specific information to the reader. We formulate this in two parts: first, what questions should the document answer for each given topic, and second, what topics should be covered. Our discussion is general and must be tailored to the circumstances of the organization.

What to Include [SZUB98] lists the following general questions that should be addressed clearly and concisely in any security policy:

- What is the reason for the policy?
- Who developed the policy?
- Who approved the policy?
- Whose authority sustains the policy?
- Which laws or regulations, if any, are the policy based on?
- Who will enforce the policy?
- How will the policy be enforced?
- Whom does the policy affect?
- What information assets must be protected?
- What are users actually required to do?
- How should security breaches and violations be reported?
- What is the effective date and expiration date of the policy?

Some of these questions are global, covering the entire document. Others need to be addressed for various topical areas.

Security Policy Topics Security involves a broad range of topics and a multitude of details. How all this material is to be addressed and organized depends on the nature of the organization and the security strategy it employs. In this subsection, we provide a typical and comprehensive list of possible topics.

The following topics are good candidates for inclusion in the security policy document:

- **Principles:** Including (a) a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing; and (b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives.
- **Organizational reporting structure:** States management commitment to information security and lists responsible individuals and offices for implementation of this security policy.
- **Physical security:** Covers physical protection of and access to all IS equipment, including servers, workstations, storage devices, and all other IS-related equipment.
- **Hiring, management, and firing:** Includes guidelines prior to employment, covering the following:
  - —Roles and responsibilities of those involved in the hiring process, relative to security
  - —Scope and limitations of background checks
  - —Explanation of terms and conditions of employment, relative to security

  Also includes guidelines during employment, covering the following:
  - —Awareness, training, and education policies
  - —Disciplinary process

  Also includes guidelines related to employee termination, covering the following:
  - —Roles and responsibilities of those involved in the termination process, relative to security
  - —Procedures for the return of assets
  - —Procedures for the removal of access rights
- **Data protection:** Covers procedures and mechanisms for data protection, including classification schemes used by the organization, data access controls, when to use encryption, and guidelines to countering industrial espionage.
- **Communications security:** Includes perimeter controls, Web usage and content filtering, e-mail usage, and telephone and fax usage.
- **Hardware:** Includes purchasing guidelines that specify required, or preferred, security features. These should supplement existing purchasing policies and guidelines.
- **Software:** Includes purchasing guidelines, list of authorized products, development standards, quality assurance and testing.

- **Operating systems:** Includes access control guidelines and logging requirements.
- **Technical support:** Discusses services offered, including help-desk functions.
- **Privacy:** Defines reasonable expectations of privacy regarding such issues as monitoring of electronic mail, logging of keystrokes, and access to users' files.
- **Access:** Defines access rights and privileges to protect assets from loss or disclosure by specifying acceptable use guidelines for users, operations staff, and management. It should provide guidelines for external connections, data communications, connecting devices to a network, and addition of new software to systems. It should also specify any required notification messages (e.g., connect messages should provide warnings about authorized usage and line monitoring and not simply say "Welcome").
- **Accountability:** Defines the responsibilities of users, operations staff, and management. It should specify an audit capability and provide incident handling guidelines (i.e., what to do and who to contact if a possible intrusion is detected).
- **Authentication:** Establishes trust through an effective password policy and by setting guidelines for remote location authentication and the use of authentication devices (e.g., one-time passwords and the devices that generate them).
- **Availability:** Defines expected availability of resources. It should address redundancy and recovery issues as well as specify operating hours and maintenance downtime periods. It should also include contact information for reporting system and network failures.
- **Maintenance:** Describes how both internal and external maintenance people are allowed to handle and access technology. One important topic to be addressed here is whether remote maintenance is allowed and how such access is controlled. Another area for consideration here is outsourcing and how it is managed.
- **Violations reporting:** Indicates which types of violations (e.g., privacy and security, internal and external) must be reported and to whom the reports are made. A nonthreatening atmosphere and the possibility of anonymous reporting will result in a greater probability that a violation will be reported if it is detected.
- **Business continuity:** Describes considerations for maintaining business continuity after various disasters and other causes of interruption; lists individuals responsible for business continuity planning and implementation.
- **Supporting information:** Provides users, staff, and management with contact information for each type of policy violation; guidelines on how to handle outside queries about a security incident or information that may be considered confidential or proprietary; and cross-references to security procedures and related information, such as company policies and governmental laws and regulations.

Organizing the Material The complete set of policies should be written clearly and concisely but must be comprehensive. Accordingly, for a medium-sized or large organization, the policy document will be daunting, especially to nontechnical staff. For this reason, it may be preferable to create a collection of documents, some of them specialized and geared to specific subsets of employees. [KABA02a] suggests the following supplementary document collection:

- General Guide for Protecting Corporate Information Assets
- Guide for Users of Portable Computers
- A Manager's Guide to Security Policies
- Human Resources and Security
- Network Administration Security Policies
- Programmer's Guide to Security and Quality Assurance
- The Operator's Security Responsibilities
- Security and the Help Desk

Each of these documents can make reference to a master policy document.

Resources for Policy Writers

An increasingly popular standard for writing and implementing security policies is **ISO 17799** (*Code of Practice for Information Security Management*). ISO 17799 is a comprehensive set of controls comprising best practices in information security. It is essentially an internationally recognized generic information security standard.

With the increasing interest in security, ISO 17799 certification, provided by various accredited bodies, has been established as a goal for many corporations, government agencies, and other organizations around the world. ISO 17799 offers a convenient framework to help security policy writers structure their policies in accordance with an international standard.

Another important set of standards is **COBIT** (Control Objectives for Information and Related Technology). This is a business-oriented set of standards for guiding management in the sound use of information technology. It has been developed as a general standard for information technology security and control practices and includes a general framework for management, users, IS audit, and security practitioners. COBIT also has a process focus and a governance flavor; that is, management's need to control and measure IT is a focus point. COBIT was developed under the auspices of a professional organization, the Information Systems Audit and Control Association (ISACA). The documents are quite detailed and provide not only a practical basis for defining security requirements but also for implementing them and verifying compliance.

Another excellent source of information is **The Standard of Good Practice for Information Security** from the Information Security Forum. The standard is designed as an aid to organizations in understanding and applying best practices for information security. Because it addresses security from a business perspective, The Standard appropriately recognizes the intersection between organizational drivers and security drivers. Appendices 14A and 14B are extracts from the standard.

In addition to these standards, a number of informal guidelines are widely consulted by organizations in developing their own security policy. The CERT Coordination Center **(www.cert.org)** has an Evaluations and Practices section of its Web site with a variety of documents and training aids related to information security for organizations. The Chief Information Officers Council **(cio.gov)** has published a collection of Best Practices and other documents related to organizational security.

14.3 EMPLOYMENT PRACTICES AND POLICIES

This section deals with personnel security: hiring, training, monitoring behavior, and handling departure. [SADO03] reports that a large majority of perpetrators of significant computer crime are individuals who have legitimate access now, or who have recently had access. Thus, managing personnel with potential access is an essential part of information security.

Employees can be involved in security violations in one of two ways. Some employees unwittingly aid in the commission of a security violation by failing to follow proper procedures, by forgetting security considerations, or by not realizing that they are creating a vulnerability. Other employees knowingly violate controls or procedures to cause or aid a security violation.

Threats from internal users include the following:

- Gaining unauthorized access or enabling others to gain unauthorized access
- Altering data
- Deleting production and backup data
- Crashing systems
- Destroying systems
- Misusing systems for personal gain or to damage the organization
- Holding data hostage
- Stealing strategic or customer data for corporate espionage or fraud schemes

Security in the Hiring Process

ISO 17799 lists the following security objective of the hiring process: to ensure that employees, contractors, and third-party users understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud, or misuse of facilities. Although we are primarily concerned in this section with employees, the same considerations apply to contractors and third-party users.

Background Checks and Screening From a security viewpoint, hiring presents management with significant challenges. [KABA02b] points out that growing evidence suggests that many people inflate their resumes with unfounded claims. Compounding this problem is the increasing reticence of former employers. Employers may hesitate to give bad references for incompetent, underperforming, or unethical employees for fear of a lawsuit if their comments become known and an employee fails to get a new job. On the other hand, a favorable reference for an employee who subsequently causes problems at his or her new job may invite a lawsuit from the new employer. As a consequence, a significant number of employers have a corporate policy that forbids discussing a former employee's performance in any way, positive or negative. The employer may limit information to the dates of employment and the title of the position held.

Despite these obstacles, employers must make a significant effort to do background checks and screening of applicants. Of course, such checks are to assure that the prospective employee is competent to perform the intended job and poses no security risk. Additionally, employers need to be cognizant of the concept of "negligent hiring" that applies in some jurisdictions. In essence, an employer may be held liable for negligent hiring if an employee causes harm to a third party (individual or company) while acting as an employee.

General guidelines for checking applicants include the following:

- Ask for as much detail as possible about employment and educational history. The more detail that is available, the more difficult it is for the applicant to lie consistently.
- Investigate the accuracy of the details to the extent reasonable.
- Arrange for experienced staff members to interview candidates and discuss discrepancies.

For highly sensitive positions, more intensive investigation is warranted. [SADO03] gives the following examples of what may be warranted in some circumstances:

- Have an investigation agency do a background check.
- Get a criminal record check of the individual.
- Check the applicant's credit record for evidence of large personal debt and the inability to pay it. Discuss problems, if you find them, with the applicant. People who are in debt should not be denied jobs: if they are, they will never be able to regain solvency. At the same time, employees who are under financial strain may be more likely to act improperly.
- Consider conducting a polygraph examination of the applicant (if legal). Although polygraph exams are not always accurate, they can be helpful if you have a particularly sensitive position to fill.
- Ask the applicant to obtain bonding for his or her position.

For many employees, these steps are excessive. However, the employer should conduct extra checks of any employee who will be in a position of trust or privileged access—including maintenance and cleaning personnel.

Employment Agreements As part of their contractual obligation, employees should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security. The agreement should include a confidentiality and nondisclosure agreement spelling out specifically that the organization's information assets are confidential unless classified otherwise and that the employee must protect that confidentiality. The agreement should also reference the organization's security policy and indicate that the employee has reviewed and agrees to abide by the policy.

During Employment

ISO 17799 lists the following security objective with respect to current employees: to ensure that employees, contractors, and third-party users are aware of information security threats and concerns and their responsibilities and liabilities with regard to information security and are equipped to support organizational security policy in the course of their normal work and to reduce the risk of human error.

Two essential elements of personnel security during employment are a comprehensive security policy document and an ongoing awareness and training program for all employees. These are covered in Sections 14.1 and 14.2.

In addition to enforcing the security policy in a fair and consistent manner, there are certain principles that should be followed for personnel security:

- **Least privilege:** Give each person the minimum access necessary to do his or her job. This restricted access is both logical (access to accounts, networks, programs) and physical (access to computers, backup tapes, and other peripherals). If every user has accounts on every system and has physical access to everything, then all users are roughly equivalent in their level of threat.
- **Separation of duties:** Carefully separate duties so that people involved in checking for inappropriate use are not also capable of making such inappropriate use. Thus, having all the security functions and audit responsibilities reside in the same person is dangerous. This practice can lead to a case in which the person may violate security policy and commit prohibited acts, yet in which no other person sees the audit trail to be alerted to the problem.
- **Limited reliance on key employees:** No one in an organization should be irreplaceable. If your organization depends on the ongoing performance of a key employee, then your organization is at risk. Organizations cannot help but have key employees. To be secure, organizations should have written policies and plans established for unexpected illness or departure. As with systems, redundancy should be built into the employee structure. There should be no single employee with unique knowledge or skills.

Termination of Employment

ISO 17799 lists the following security objective with respect to termination of employment: to ensure that employees, contractors, and third-party users exit an organization or change employment in an orderly manner, and that the return of all equipment and the removal of all access rights are completed.

The termination process is complex and depends on the nature of the organization, the status of the employee in the organization, and the reason for departure. From a security point of view, the following actions are important:

- Removing the person's name from all lists of authorized access
- Explicitly informing guards that the ex-employee is not allowed into the building without special authorization by named employees
- Removing all personal access codes
- If appropriate, changing lock combinations, reprogramming access card systems, and replacing physical locks
- Recovering all assets, including employee ID, disks, documents, and equipment

14.4 E-MAIL AND INTERNET USE POLICIES

E-mail and Internet access for most or all employees is common in office environments and is typically provided for at least some employees in other environments, such as a factory. A growing number of companies incorporate specific e-mail and Internet use policies into the organization's security policy document. This section examines some important considerations for these policies.

Motivation

Widespread use of e-mail and the Internet by employees raises a number of concerns for employers, including the following:

1. Significant employee work time may be consumed in non-work-related activities, such as surfing the Web, playing games on the Web, shopping on the Web, chatting on the Web, and sending and reading personal e-mail.
2. Significant computer and communications resources may be consumed by such non-work-related activity, compromising the mission that the IS resources are designed to support.
3. Excessive and casual use of the Internet and e-mail unnecessarily increases the risk of introduction of malicious software into the organization's IS environment.
4. The non-work-related employee activity could result in harm to other organizations or individuals outside the organization, thus creating a liability for the organization.
5. E-mail and the Internet may be used as tools of harassment by one employee against another.
6. Inappropriate online conduct by an employee may damage the reputation of the organization.

Policy Issues

The development of a comprehensive e-mail and Internet use policy raises a number of policy issues. The following is a suggested set of policies, based on [KING06].

- **Business use only:** Company-provided e-mail and Internet access are to be used by employees only for the purpose of conducting company business.
- **Policy scope:** Policy covers e-mail access; contents of e-mail messages; Internet and intranet communications; and records of e-mail, Internet, and intranet communications.
- **Content ownership:** Electronic communications, files, and data remain company property even when transferred to equipment not owned by the company.
- **Privacy:** Employees have no expectation of privacy in their use of company-provided e-mail or Internet access, even if the communication is personal in nature.

- **Standard of conduct:** Employees are expected to use good judgment and act courteously and professionally when using company-provided e-mail and Internet access.
- **Reasonable personal use:** Employees may make reasonable personal use of company-provided e-mail and Internet access provided that such use does not interfere with the employee's duties, violate company policy, or unduly burden company facilities.
- **Unlawful activity prohibited:** Employees may not use company-provided e-mail and Internet access for any illegal purpose.
- **Security policy:** Employees must follow the company's security policy when using e-mail and Internet access.
- **Company policy:** Employees must follow all other company policies when using e-mail and Internet access. Company policy prohibits viewing, storing, or distributing pornography; making or distributing harassing or discriminatory communications; and unauthorized disclosure of confidential or proprietary information.
- **Company rights:** The company may access, monitor, intercept, block access, inspect, copy, disclose, use, destroy, recover using computer forensics, and/or retain and communications, files, or other data covered by this policy. Employees are required to provide passwords upon request.
- **Disciplinary action:** Violation of this policy may result in immediate termination of employment or other discipline deemed appropriate by the company.

Guidelines for Developing a Policy

A useful document to consult when developing an e-mail and Internet use policy is *Guidelines to Assist Agencies in Developing Email and Internet Use Policies*, from the Office of e-Government, of the Government of Western Australia, July 2004. A copy is available at this book's Web site.

14.5 EXAMPLE: A CORPORATE SECURITY POLICY DOCUMENT

To give the reader a feel for how organizations deal with physical security, we provide a real-world example of a security policy document. The company is an EU-based engineering consulting firm that specializes in the provision of planning, design, and management services for infrastructure development worldwide. With interests in transportation, water, maritime, and property, the company is undertaking commissions in over 70 countries from a network of more than 70 offices.

Figure 14.3 is the table of contents of the company's security standards document. For our purposes, we have changed the name of the company to Company wherever it appears in the document. The table of contents indicates the topical scope of the document. As an illustration of the level of detail, Figure 13.3 reproduces Section 5 of the document, covering physical and environmental security. The entire document is available at this book's Web site.

COMPANY SECURITY POLICY—INDEX

Executive Summary

1. **Security Policy**
   - 1.1. Security Policy Documents
   - 1.2. Review and Evaluation
2. **Company Security**
   - 2.1. Information security infrastructure
   - 2.2. Security of third party access
   - 2.3. Outsourcing
   - 2.4. Partnerships, Joint ventures and Alliances
3. **Asset classification and control**
   - 3.1. Accountability for assets
   - 3.2. Fraud policy
   - 3.3. Information classification
   - 3.4. Asset Protection
4. **Personnel security**
   - 4.1. Security in job definition and resourcing
   - 4.2. User training
   - 4.3. Responding to security incidents and malfunctions
   - 4.4. Joiners, Leavers and Travellers
5. **Physical and Environmental security**
   - 5.1. Secure Areas
   - 5.2. Equipment Security
   - 5.3. General Controls
6. **Communications and operations management**
   - 6.1. Operational procedures and responsibilities
   - 6.2. System planning and acceptance
   - 6.3. Protection against malicious software
   - 6.4. Housekeeping
   - 6.5. Network management
   - 6.6. Media handling and security
   - 6.7. Exchanges of information and software
7. **Logical Access control**
   - 7.1. Business requirement for access control
   - 7.2. User access management
   - 7.3. User responsibilities
   - 7.4. Network access control
   - 7.5. Operating system access control
   - 7.6. Application access control
   - 7.7. Monitoring system access and use
   - 7.8. Mobile computing and Teleworking
   - 7.9. Internet/Intranet access
8. **Development and Maintenance**
   - 8.1. Security Requirements
   - 8.2. Security in Application Systems
   - 8.3. Cryptographic Controls
   - 8.4. Security of system files
   - 8.5. Security in Development and support processes
   - 8.6. Security During Maintenance
9. **Business Continuity Management**
   - 9.1. Aspects of Business Continuity Management

Figure 14.3 **The Company's Security Policy—Table of Contents**

10. **Compliance**
  10.1. Compliance with Legal Requirements
  10.2. Review of security policy and technical compliance
  10.3. Audit Consideration
A **Annex A — Mutual Confidentiality Agreement**
B **Annex B — Personal Acceptance Document**
C **Annex C — Code of Connection**
  C.1 Background
  C.2 Principle of Connection
  C.3 End System Security Policies
  C.4 Company Voice and Data Networks Security Requirements

Figure 14.3 *(Continued)*

14.6 RECOMMENDED READING AND WEB SITES

[WILS98] is a lengthy treatment of security training. [BOWE06], [NIST95], and [SZUB98] each has a useful chapter on security awareness, training, and education. [MCGO02] and [SIPO01] are useful articles on security awareness; [WYK06] covers training.

[NIST95], [FRAS97], [SADO03], and [SZUB98] each contain useful chapters on organizational security policies.

BOWE06 Bowen, P.; Hash, J.; and Wilson, M. *Information Security Handbook: A Guide for Managers.* NIST Special Publication 800-100. October 2006.

FRAS97 Fraser, B. *Site Security Handbook.* RFC 2196, September 1997.

MCGO02 McGovern, M. "Opening Eyes: Building Company-Wide IT Security Awareness." *IT Pro*, May/June 2002.

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

SADO03 Sadowsky, G., et al. *Information Technology Security Handbook.* Washington, DC: The World Bank, 2003. http://www.infodev-security.net/handbook

SIPO01 Siponen, N. "Five Dimensions of Information Security Awareness." *Computers and Society*, June 2001.

SZUB98 Szuba, T. *Safeguarding Your Technology.* National Center for Education Statistics, NCES 98-297, 1998. nces.ed.gov/pubsearch/pubsinfo.asp?pubid=98297

WILS98 Wilson, M., ed. *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* NIST Special Publication 800-16. April 1998.

WYK06 Wyk, K., and Steven, J. "Essential Factors for Successful Software Security Awareness Training." *IEEE Security and Privacy*, September/October 2006.

Recommended Web sites:

- **Federal Agency Security Practices:** A voluminous set of documents covering all aspects of organizational security policy
- **ISO 17799 Community Portal:** Documents, links, and other resources related to ISO 17799

14.7 KEY TERMS, REVIEW QUESTIONS, AND PROBLEMS

Key Terms

COBIT e-mail and Internet use policy	ISO 17799 security awareness security education	security policy security training

Review Questions

14.1 What are the benefits of a security awareness, training, and education program for an organization?

14.2 What is the difference between security awareness and security training?

14.3 What is an organizational security policy?

14.4 Who should be involved in developing the organization's security policy and its security policy docment?

14.5 What is ISO 17799?

14.6 What principles should be followed in designing personnel security policies?

14.7 Why is an e-mail and Internet use policy needed?

Problems

14.1 Section 14.1 includes a quotation from SP-800-100 to the effect that awareness deals with the what but not the how of security. Explain the distinction in this context.

14.2 **a.** Joe the janitor is recorded on the company security camera one night taking pictures with his cell phone of the office of the CEO after he is done cleaning it. The film is grainy (from repeated use and reuse) and you cannot ascertain what specifically he is taking pictures of. You can see the flash of his cell phone camera going off and you note that the flash is coming from the area directly in front of the CEO's desk. What will you do and what is your justification for your actions?

b. What can you do in the future to prevent or at least mitigate any legal challenges that Joe the janitor may bring to court?

14.3 During a routine check of Ozzie's work computer, you note that the checksums of his screensaver pictures have been modified slightly. What actions, if any, do you take?

14.4 You observe Lynsay with a "keychain portstick" (USB port, fingerstick) one morning as she is coming into work. What do you do?

14.5 Harriet's workstation computer reveals the installation of a game called Bookworm. What actions do you take before confronting Harriet? Why?

14.6 Phil maintains a blog online. What do you do to check that his blog is not revealing sensitive company information? Is he allowed to maintain his blog during work hours? He argues that his blog is something he does when not at work. How do you respond? You discover that his blog contains a link to the site YourCompanySucks. Phil states he is not the author of that site. Now what do you do?

APPENDIX 14A SECURITY AWARENESS STANDARD OF GOOD PRACTICE

These specifications are from *The Standard of Good Practice for Information Security* [ISF05].

Security Management

Focus: Security management at the enterprise level

Principle: Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the enterprise.

Objective: To ensure all relevant individuals understand the key elements of information security and why it is needed, and understand their personal information security responsibilities.

1. Specific activities should be performed to promote security awareness (the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities—and act accordingly) across the enterprise. These activities should be:
   a. endorsed by top management
   b. the responsibility of a particular individual, organisational unit, working group or committee
   c. supported by a documented set of objectives
   d. delivered as part of an on-going security awareness programme
   e. subject to project management disciplines
   f. kept up-to-date with current practices and requirements
   g. based on the results of a risk assessment
   h. aimed at reducing the frequency and magnitude of incidents
   i. measurable.
2. Security awareness should be promoted:
   a. to top management, business managers/users, IT staff and external personnel
   b. by providing information security education/training, such as via computer-based training (CBT)
   c. by supplying specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.
3. Staff should be provided with guidance to help them understand:
   a. the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
   b. the importance of complying with information security policy and applying associated standards/procedures
   c. their personal responsibilities for information security.
4. The effectiveness of security awareness should be monitored by measuring:
   a. the level of security awareness in staff and reviewing it periodically
   b. the effectiveness of security awareness activities, for example by monitoring the frequency and magnitude of incidents experienced.
5. Security-positive behaviour should be encouraged by:
   a. making attendance at security awareness training compulsory
   b. publicising security successes and failures throughout the organisation
   c. linking security to personal performance objectives/appraisals.

Critical Business Applications

Focus: A business application that is critical to the success of the enterprise

Principle: Users of the application should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure users of the application apply security controls and prevent the security of information used in the application from being compromised.

1. Users of the application should be covered by an information security policy. They should be aware of the policy and comply with it.
2. Users of the application should:
   a. take part in a security awareness programme (security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities—and act accordingly)
   b. be provided with information security education/training, such as via computer-based training (CBT)
   c. be supplied with specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.
3. Users of the application should be made aware of:
   a. the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
   b. why information security is needed to protect the application
   c. the importance of complying with information security policies and applying associated standards/procedures
   d. their personal responsibilities for information security.
4. Users of the application should be made aware that they are prohibited from:
   a. using information or systems without authorisation
   b. using the application for purposes that are not work-related
   c. making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
   d. making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
   e. downloading illegal material (e.g. with obscene or discriminatory content)
   f. using unauthorised application components (e.g. installing unauthorised third party software or modems)
   g. unauthorised copying of information or software
   h. disclosing confidential information (e.g. customer records, product designs and pricing policies)
   i. compromising passwords (e.g. by writing them down or disclosing them to others)
   j. using personally identifiable information for business purposes unless explicitly authorised
   k. tampering with evidence in the case of incidents that may require forensic investigation.
5. Users of the application should be warned of the dangers of being overheard when discussing business information either over the telephone or in public places (e.g. train carriages, airport lounges or bars).

Computer Installations

Focus: A computer installation that supports one or more business applications

Principle: Staff running the installation should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure that staff running the installation apply security controls and prevent the security of information used in the computer installation from being compromised.

1. There should be an information security policy that applies to the computer installation. Staff employed in the computer installation should be aware of the policy and comply with it.
2. Staff employed in the computer installation should:
   a. take part in a security awareness programme (security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities–and act accordingly)
   b. be provided with information security education/training, such as via computer-based training (CBT)
   c. be supplied with specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.
3. Staff employed in the computer installation should be made aware of:
   a. the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
   b. why information security is needed to protect the installation
   c. the importance of complying with information security policies and applying associated standards/procedures
   d. their personal responsibilities for information security.
4. Staff employed in the computer installation should be made aware that they are prohibited from:
   a. using any part of the installation without authorisation or for purposes that are not work-related
   b. making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
   c. making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
   d. downloading illegal material (e.g. with obscene or discriminatory content)
   e. using unauthorised installation components (e.g. installing unauthorised third party software or modems)
   f. unauthorised copying of information or software
   g. disclosing confidential information (e.g. customer records, product designs or pricing policies)
   h. compromising passwords (e.g. by writing them down or disclosing them to others)
   i. using personally identifiable information for business purposes unless explicitly authorised
   j. tampering with evidence in the case of incidents that may require forensic investigation.

Networks

Focus: A network that supports one or more business application

Principle: Network staff should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure network staff apply security controls and prevent the security of information transmitted across the network from being compromised.

1. There should be an information security policy that applies to the network. Network staff should be aware of the policy and comply with it.
2. Network staff should:
    a. take part in a security awareness programme (security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities—and act accordingly)
    b. be provided with information security education/training, such as via computer-based training (CBT)
    c. be supplied with specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.
3. Network staff should be made aware of:
    a. the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
    b. why information security is needed to protect the network
    c. the importance of complying with information security policies and applying associated standards/procedures
    d. their personal responsibilities for information security.
4. Network staff should be made aware that they are prohibited from:
    a. using any part of the network without authorisation or for purposes that are not work-related
    b. making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
    c. making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
    d. downloading illegal material (e.g. with obscene or discriminatory content)
    e. using unauthorised network components (e.g. installing unauthorised third party software or modems)
    f. unauthorised copying of information or software
    g. disclosing confidential information (e.g. network designs or IP addresses)
    h. compromising passwords (e.g. by writing them down or disclosing them to others)
    i. using personally identifiable information for business purposes unless explicitly authorised
    j. tampering with evidence in the case of incidents that may require forensic investigation.

Systems Development

Focus: A systems development unit/department or a particular systems development project.

Principle: Systems development staff should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure systems development staff apply security controls and prevent the security of information used in development activities from being compromised.

1. There should be an information security policy that applies to development activities. Development staff should be aware of the policy and comply with it.
2. Development staff should:
   - a. take part in a security awareness programme (security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities — and act accordingly)
   - b. be provided with information security education/training, such as via computer-based training (CBT)
   - c. be supplied with specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.
3. Development staff should be made aware of:
   - a. the meaning of information security (i.e. the protection of the confidentiality, integrity and availability of information)
   - b. why information security is needed to protect systems development activities
   - c. the importance of complying with information security policies and applying associated standards/procedures
   - d. their personal responsibilities for information security.
4. Development staff should be made aware that they are prohibited from:
   - a. using information or systems without authorisation or for purposes that are not work-related
   - b. making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
   - c. making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
   - d. downloading illegal material (e.g. with obscene or discriminatory content)
   - e. using unauthorised system components (e.g. installing unauthorised third party software or modems)
   - f. unauthorised copying of information or software
   - g. disclosing confidential information (e.g. development designs, IP addresses or details of external connections)
   - h. compromising passwords (e.g. writing them down or disclosing them to others)
   - i. using personally identifiable information for business purposes unless explicitly authorised
   - j. tampering with evidence in the case of incidents that may require forensic investigation.

APPENDIX 14B SECURITY POLICY STANDARD OF GOOD PRACTICE

This specification is from *The Standard of Good Practice for Information Security* [ISF05].

Principle: A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the enterprise's information and systems.

Objective: To document top management's direction on and commitment to information security, and communicate it to all relevant individuals.

1. There should be a documented information security policy, ratified at top level, that applies across the enterprise. There should be an individual (or a group of individuals) responsible for maintaining the policy.

2. The information security policy should define information security, associated responsibilities and the information security principles to be followed by all staff.

3. The information security policy should require:
   a. critical information and systems to be subjected to a risk analysis on a regular basis
   b. that an "owner"—typically the person in charge of a particular business application, computer installation or network—is assigned for all critical information and systems
   c. that information and systems are classified in a way that indicates their criticality to the enterprise
   d. that staff are made aware of information security
   e. compliance with software licenses and with legal, regulatory and contractual obligations
   f. breaches of the security policy and suspected security weaknesses to be reported
   g. information to be protected in terms of its requirements for confidentiality, integrity and availability.

4. A high level policy (e.g. the information security policy) should prohibit:
   a. using the enterprise's information and systems without authorization or for purposes that are not work-related
   b. making sexual, racist or other statements, which may be offensive (e.g. by using e-mail or the Internet)
   c. making obscene, discriminatory or harassing statements, which may be illegal (e.g. by using e-mail or the Internet)
   d. downloading illegal material (e.g. with obscene or discriminatory content)
   e. the movement of information or equipment off-site without authorization
   f. unauthorized use of information, facilities or equipment
   g. unauthorized copying of information/software
   h. compromising passwords (e.g. by writing them down or disclosing them to others)
   i. using personally identifiable information for business purposes unless explicitly authorized
   j. discussing business information in public places
   k. tampering with evidence in the case of an incident.

5. A high level policy (e.g. the information security policy) should state that users should:
   a. lock away sensitive media or documentation when not in use (i.e. complying with a "clear desk" policy)
   b. log-off systems in use when leaving a terminal/workstation unattended (e.g. during a meeting, lunch break or overnight).

6. The information security policy should be:
   a. communicated to all staff and external parties with access to the enterprise's information or systems
   b. reviewed regularly according to a defined review process
   c. revised to take account of changing circumstances.

7. The information security policy should state that disciplinary actions may be taken against individuals who violate its provisions.