chapter 3

Operational and Organizational Security

We will bankrupt ourselves in the vain search for absolute security.

—Dwight David Eisenhower

In this chapter, you will learn how to

- Identify various operational aspects to security in your organization
- Identify various policies and procedures in your organization
- Identify the security awareness and training needs of an organization
- Understand the different types of agreements employed in negotiating security requirements
- Describe the physical security components that can protect your computers and network
- Identify environmental factors that can affect security
- Identify factors that affect the security of the growing number of wireless technologies used for data transmission
- Prevent disclosure through electronic emanations

Organizations achieve operational security through policies and procedures that guide user's interactions with data and data processing systems. Developing and aligning these efforts with the goals of the business is a crucial part of developing a successful security program. One method of ensuring coverage is to align efforts with the operational security model described in the last chapter. This breaks efforts into groups; prevention, detection, and response elements.

Prevention technologies are designed to keep individuals from being able to gain access to systems or data they are not authorized to use. Originally, this was the sole approach to security. Eventually we learned that in an operational environment, prevention is extremely difficult and relying on prevention technologies alone is not sufficient. This led to the rise of technologies to detect and respond to events that occur when prevention fails. Together, the prevention technologies and the detection and response technologies form the operational model for computer security.

Policies, Procedures, Standards, and Guidelines

These documents guide how security will be implemented in the organization:

Policies High-level, broad statements of what the organization wants to accomplish

Procedures Step-by-step instructions on how to implement the policies

Standards Mandatory elements regarding the implementation of a policy

Guidelines Recommendations relating to a policy

An important part of any organization's approach to implementing security are the policies, procedures, standards, and guidelines that are established to detail what users and administrators should be doing to maintain the security of the systems and network. Collectively, these documents provide the guidance needed to determine how security will be implemented in the organization. Given this guidance, the specific technology and security mechanisms required can be planned for.

Policies are high-level, broad statements of what the organization wants to accomplish. They are made by management when laying out the organization's position on some issue. **Procedures** are the step-by-step instructions on how to implement policies in the organization. They describe exactly how employees are expected to act in a given situation or to accomplish a specific task. **Standards** are mandatory elements regarding the implementation of a policy. They are accepted specifications that provide specific details on how a policy is to be enforced. Some standards are externally driven. Regulations for banking and financial institutions, for example, require certain security measures be taken by law. Other standards may be set by the organization to meet its own security goals. **Guidelines** are recommendations relating to a policy. The key term in this case is *recommendations*—guidelines are not mandatory steps.

Just as the network itself constantly changes, the policies, procedures, standards, and guidelines should be included in living documents that are periodically evaluated and changed as necessary. The constant monitoring of the network and the periodic review of the relevant documents are part of the process that is the operational model. When applied to policies, this process results in what is known as the *policy lifecycle.* This operational process and policy lifecycle roughly consist of four steps in relation to your security policies and solutions:

1. Plan (adjust) for security in your organization.
2. Implement the plans.
3. Monitor the implementation.
4. Evaluate the effectiveness.

In the first step, you develop the policies, procedures, and guidelines that will be implemented and design the security components that will protect your network. There are a variety of governing instruments, from standards to compliance rules that will provide boundaries for these documents. Once these documents are designed and developed, you can implement the plans. Part of the implementation of any policy, procedure, or guideline is an instruction period during which those who will be affected by the change or introduction of this new document learn about its contents. Next, you monitor to ensure that both the hardware and the software as well as the policies, procedures, and guidelines are effective in securing your systems. Finally, you evaluate the effectiveness of the security measures you have in place. This step may include a *vulnerability assessment* (an attempt to identify and prioritize the list of vulnerabilities within a system

or network) and a *penetration test* (a method to check the security of a system by simulating an attack by a malicious individual) of your system to ensure the security is adequate. After evaluating your security posture, you begin again with step one, this time adjusting the security mechanisms you have in place, and then continue with this cyclical process.

Regarding security, every organization should have several common policies in place (in addition to those already discussed relative to access control methods). These include, but are not limited to, security policies regarding change management, classification of information, acceptable use, due care and due diligence, due process, need to know, disposal and destruction of data, service level agreements, human resources issues, codes of ethics, and policies governing incident response.

Security Policies

In keeping with the high-level nature of policies, the **security policy** is a high-level statement produced by senior management that outlines both what security means to the organization and the organization's goals for security. The main security policy can then be broken down into additional policies that cover specific topics. Statements such as "this organization will exercise the principle of least access in its handling of client information" would be an example of a security policy. The security policy can also describe how security is to be handled from an organizational point of view (such as describing which office and corporate officer or manager oversees the organization's security program).

In addition to policies related to access control, the organization's security policy should include the specific policies described in the next sections. All policies should be reviewed on a regular basis and updated as needed. Generally, policies should be updated less frequently than the procedures that implement them, since the high-level goals will not change as often as the environment in which they must be implemented. All policies should be reviewed by the organization's legal counsel, and a plan should be outlined that describes how the organization will ensure that employees will be made aware of the policies. Policies can also be made stronger by including references to the authority who made the policy (whether this policy comes from the CEO or is a department-level policy, for example) and references to any laws or regulations that are applicable to the specific policy and environment.

Change Management Policy

The purpose of *change management* is to ensure proper procedures are followed when modifications to the IT infrastructure are made. These modifications can be prompted by a number of different events, including new legislation, updated versions of software or hardware, implementation of new software or hardware, or improvements to the infrastructure. The term "management" implies that this process should be controlled in some systematic way, and that is indeed the purpose. Changes to the infrastructure might have a detrimental impact on operations. New versions of operating systems or application software might be incompatible with other software or hardware the organization is using. Without a process to manage

the change, an organization might suddenly find itself unable to conduct business. A change management process should include various stages, including a method to request a change to the infrastructure, a review and approval process for the request, an examination of the consequences of the change, resolution (or mitigation) of any detrimental effects the change might incur, implementation of the change, and documentation of the process as it related to the change.

Data Policies

System integration with third parties frequently involves the sharing of data. Data can be shared for the purpose of processing or storage. Control over data is a significant issue in third-party relationships. There are numerous questions that need to be addressed. The question of who owns the data, both the data shared with third parties and subsequent data developed as part of the relationship, is an issue that needs to be established.

Data Ownership

Data requires a data owner. Data ownership roles for all data elements need to be defined in the business. Data ownership is a business function, where the requirements for security, privacy, retention, and other business functions must be established. Not all data requires the same handling restrictions, but all data requires these characteristics to be defined. This is the responsibility of the data owner.

Unauthorized Data Sharing

Unauthorized data sharing can be a significant issue, and in today's world, data has value and is frequently used for secondary purposes. Ensuring that all parties in the relationship understand the data-sharing requirements is an important prerequisite. Equally important is ensuring that all parties understand the security requirements of shared data.

Data Backups

Data ownership requirements include backup responsibilities. Data backup requirements include determining the level of backup, restore objectives, and level of protection requirements. These can be defined by the data owner and then executed by operational IT personnel. Determining the backup responsibilities and developing the necessary operational procedures to ensure that adequate backups occur are important security elements.

Classification of Information

A key component of IT security is the protection of the information processed and stored on the computer systems and network. Organizations deal with many different types of information, and they need to recognize that not all information is of equal importance or sensitivity. This requires classification of information into various categories, each with its own requirements for its handling. Factors that affect the classification of specific information include its value to the organization (what will be the impact to the organization if it loses this information?), its age, and laws or

Tech Tip

Data Classification

Information classification categories you should be aware of for the CompTIA Security+ exam include: High, Medium, Low, Confidential, Private, and Public.

regulations that govern its protection. The most widely known system of classification of information is that implemented by the U.S. government (including the military), which classifies information into categories such as *Confidential*, *Secret*, and *Top Secret*. Businesses have similar desires to protect information and often use categories such as *Publicly Releasable*, *Proprietary*, *Company Confidential*, and *For Internal Use Only*. Each policy for the classification of information should describe how it should be protected, who may have access to it, who has the authority to release it and how, and how it should be destroyed. All employees of the organization should be trained in the procedures for handling the information that they are authorized to access. Discretionary and mandatory access control techniques use classifications as a method to identify who may have access to what resources.

Data Labeling, Handling, and Disposal

Effective data classification programs include data labeling, which enables personnel working with the data to know whether it is sensitive and to understand the levels of protection required. When the data is inside an information-processing system, the protections should be designed into the system. But when the data leaves this cocoon of protection, whether by printing, downloading, or copying, it becomes necessary to ensure continued protection by other means. This is where data labeling assists users in fulfilling their responsibilities. Training to ensure that labeling occurs and that it is used and followed is important for users whose roles can be impacted by this material.

Training plays an important role in ensuring proper data handling and disposal. Personnel are intimately involved in several specific tasks associated with data handling and data destruction/disposal and, if properly trained, can act as a security control. Untrained or inadequately trained personnel will not be a productive security control and, in fact, can be a source of potential compromise.

Need to Know

Another common security principle is that of *need to know*, which goes hand-in-hand with *least privilege*. The guiding factor here is that each individual in the organization is supplied with only the absolute minimum amount of information and privileges he or she needs to perform their work tasks. To obtain access to any piece of information, the individual must have a justified need to know. A policy spelling out these two principles as guiding philosophies for the organization should be created. The policy should also address who in the organization can grant access to information and who can assign privileges to employees.

Disposal and Destruction Policy

Many potential intruders have learned the value of dumpster diving. An organization must be concerned about not only paper trash and discarded objects, but also the information stored on discarded objects such as computers. Several government organizations have been embarrassed when old computers sold to salvagers proved to contain sensitive documents on their hard drives. It is critical for every organization to have a strong *disposal and destruction policy* and related procedures.

Important papers should be shredded, and *important* in this case means anything that might be useful to a potential intruder. It is amazing what intruders can do with what appear to be innocent pieces of information.

Before magnetic storage media (such as disks or tapes) is discarded in the trash or sold for salvage, it should have all files deleted, and should be overwritten at least three times with all 1's, all 0's, and then random characters. Commercial products are available to destroy files using this process. It is not sufficient simply to delete all files and leave it at that, since the deletion process affects only the pointers to where the files are stored and doesn't actually get rid of all the bits in the file. This is why it is possible to "undelete" files and recover them after they have been deleted.

A safer method for destroying files from a storage device is to destroy the data magnetically, using a strong magnetic field to *degauss* the media. This effectively destroys all data on the media. Several commercial degaussers are available for this purpose. Another method that can be used on hard drives is to use a file on them (the sort of file you'd find in a hardware store) and actually file off the magnetic material from the surface of the platter. Shredding floppy media is normally sufficient, but simply cutting a floppy disk into a few pieces is not enough—data has been successfully recovered from floppies that were cut into only a couple of pieces. CDs and DVDs also need to be disposed of appropriately. Many paper shredders now have the ability to shred these forms of storage media. In some highly secure environments, the only acceptable method of disposing of hard drives and other storage devices is the actual physical destruction of the devices. Matching the security action to the level of risk is important to recognize in this instance. Destroying hard drives that do not have sensitive information is wasteful; proper file scrubbing is probably appropriate. For drives with ultra-sensitive information, physical destruction makes sense. There is no single answer, but as in most things associated with information security, the best practice is to match the action to the level of risk.

Human Resources Policies

It has been said that the weakest links in the security chain are the humans. Consequently, it is important for organizations to have policies in place relative to their employees. Policies that relate to the hiring of individuals are primarily important. The organization needs to make sure that it hires individuals who can be trusted with the organization's data and that of its clients. Once employees are hired, they should be kept from slipping into the category of "disgruntled employee." Finally, policies must be developed to address the inevitable point in the future when an employee leaves the organization—either on his or her own or with the "encouragement" of the organization itself. Security issues must be considered at each of these points.

Many organizations overlook the security implications that decisions by Human Resources may have. Human Resources personnel and security personnel should have a close working relationship. Decisions on the hiring and firing of personnel have direct security implications for the organization. As a result, procedures should be in place that specify which actions must be taken when an employee is hired, is terminated, or retires.

Code of Ethics

Numerous professional organizations have established codes of ethics for their members. Each of these describes the expected behavior of their members from a high-level standpoint. Organizations can adopt this idea as well. For organizations, a code of ethics can set the tone for how employees will be expected to act and to conduct business. The code should demand

honesty from employees and require that they perform all activities in a professional manner. The code could also address principles of privacy and confidentiality and state how employees should treat client and organizational data. Conflicts of interest can often cause problems, so this could also be covered in the code of ethics.

By outlining a code of ethics, the organization can encourage an environment that is conducive to integrity and high ethical standards. For additional ideas on possible codes of ethics, check professional organizations such as the Institute for Electrical and Electronics Engineers (IEEE), the Association for Computing Machinery (ACM), or the Information Systems Security Association (ISSA).

Job Rotation

An interesting approach to enhance security that is gaining increasing attention is *job rotation.* Organizations often discuss the benefits of rotating individuals through various jobs in an organization's IT department. By rotating through jobs, individuals gain a better perspective on how the various parts of IT can enhance (or hinder) the business. Since security is often a misunderstood aspect of IT, rotating individuals through security positions can result in a much wider understanding throughout the organization about potential security problems. It also can have the side benefit of a company not having to rely on any one individual too heavily for security expertise. If all security tasks are the domain of one employee, and that individual leaves suddenly, security at the organization could suffer. On the other hand, if security tasks are understood by many different individuals, the loss of any one individual has less of an impact on the organization.

Employee Hiring and Promotions

It is becoming common for organizations to run background checks on prospective employees and to check the references prospective employees supply. Frequently, organizations require drug testing, check for any past criminal activity, verify claimed educational credentials, and confirm reported work history. For highly sensitive environments, special security background investigations can also be required. Make sure that your organization hires the most capable and trustworthy employees, and that your policies are designed to ensure this.

After an individual has been hired, your organization needs to minimize the risk that the employee will ignore company rules and affect security. Periodic reviews by supervisory personnel, additional drug checks, and monitoring of activity during work may all be considered by the organization. If the organization chooses to implement any of these reviews, this must be specified in the organization's policies, and prospective employees should be made aware of these policies before being hired. What an organization can do in terms of monitoring and requiring drug tests, for example, can be severely restricted if not spelled out in advance as terms of employment. New hires should be made aware of all pertinent policies, especially those applying to security, and should be asked to sign documents indicating that they have read and understood them.

Occasionally an employee's status will change within the company. If the change can be construed as a negative personnel action (such as a demotion), supervisors should be alerted to watch for changes in behavior that

Tech Tip

Hiring Hackers

Hiring a skilled hacker may make sense from a technical skills point of view, but an organization also has to consider the broader ethical and business consequences and associated risks. Is the hacker completely reformed or not? How much time is needed to determine this? The real question is not "Would you hire a hacker?" but rather "Can you fire a hacker once he has had access to your systems?" Trust is an important issue with employees who have system administrator access, and the long-term ramifications need to be considered.

Tech Tip

Accounts of Former Employees

When conducting security assessments of organizations, security professionals frequently find active accounts for individuals who no longer work for the company. This is especially true for larger organizations, which may lack a clear process for the personnel office to communicate with the network administrators when an employee leaves the organization. These old accounts, however, are a weak point in the security perimeter for the organization and should be eliminated.

might indicate the employee is contemplating or conducting unauthorized activity. It is likely that the employee will be upset, and whether he acts on this to the detriment of the company is something that needs to be guarded against. In the case of a demotion, the individual may also lose certain privileges or access rights, and these changes should be made quickly so as to lessen the likelihood that the employee will destroy previously accessible data if he becomes disgruntled and decides to take revenge on the organization. On the other hand, if the employee is promoted, privileges may still change, but the need to make the change to access privileges may not be as urgent, though it should still be accomplished as quickly as possible. If the move is a lateral one, changes may also need to take place, and again they should be accomplished as quickly as possible.

Retirement, Separation, or Termination of an Employee

An employee leaving an organization can be either a positive or a negative action. Employees who are retiring by their own choice may announce their planned retirement weeks or even months in advance. Limiting their access to sensitive documents the moment they announce their intention may be the safest thing to do, but it might not be necessary. Each situation should be evaluated individually. If the situation is a forced retirement, the organization must determine the risk to its data if the employee becomes disgruntled as a result of the action. In this situation, the wisest choice might be to cut off the employee's access quickly and provide her with some additional vacation time. This might seem like an expensive proposition, but the danger to the company of having a disgruntled employee may justify it. Again, each case should be evaluated individually.

It is better to give a potentially disgruntled employee several weeks of paid vacation than to have him trash sensitive files to which he has access. Because employees typically know the pattern of management behavior with respect to termination, doing the right thing will pay dividends in the future for a firm.

When an employee decides to leave a company, generally as a result of a new job offer, continued access to sensitive information should be carefully considered. If the employee is leaving as a result of hard feelings toward the company, it might be wise to quickly revoke her access privileges.

If the employee is leaving the organization because he is being terminated, you should assume that he is or will become disgruntled. While it may not seem the friendliest thing to do, an employee in this situation should immediately have his access privileges to sensitive information and facilities revoked.

Combinations should also be quickly changed once an employee has been informed of their termination. Access cards, keys, and badges should be collected; the employee should be escorted to her desk and watched as she packs personal belongings; and then she should be escorted from the building.

Organizations commonly neglect to have a policy that mandates the removal of an individual's computer access upon termination. Not only should such a policy exist, but it should also include the procedures to reclaim and "clean" a terminated employee's computer system and accounts.

Mandatory Vacations

Organizations have provided vacation time to their employees for many years. Few, however, force employees to take this time if they don't want to. At some companies, employees are given the choice to either "use or lose" their vacation time; if they do not take all of their vacation time, they lose at least a portion of it. From a security standpoint, an employee who never takes time off might be involved in nefarious activity, such as fraud or embezzlement, and might be afraid that if he leaves on vacation, the organization will discover his illicit activities. As a result, requiring employees to use their vacation time through a policy of mandatory vacations can be

a security protection mechanism. Using mandatory vacations as a tool to detect fraud will require that somebody else also be trained in the functions of the employee who is on vacation. Having a second person familiar with security procedures is also a good policy in case something happens to the primary employee.

On-boarding/Off-boarding Business Partners

Just as it is important to manage the on- and off-boarding processes of company personnel, it is important to consider the same types of elements when making arrangements with third parties. Agreements with business partners tend to be fairly specific with respect to terms associated with mutual expectations associated with the process of the business. Considerations regarding the on-boarding and off-boarding processes are important, especially the off-boarding. When a contract arrangement with a third party comes to an end, issues as to data retention and destruction by the third party need to be addressed. These considerations need to be made prior to the establishment of the relationship, not added at the time that it is coming to an end.

On-boarding and off-boarding business procedures should be well documented to ensure compliance with legal requirements.

Social Media Networks

The rise of social media networks has changed many aspects of business. Whether used for marketing, communications, customer relations, or some other purpose, social media networks can be considered a form of third party. One of the challenges in working with social media networks and/or applications is their terms of use. While a relationship with a typical third party involves a negotiated set of agreements with respect to requirements, there is no negotiation with social media networks. The only option is to adopt their terms of service, so it is important to understand the implications of these terms with respect to the business use of the social network.

Acceptable Use Policy

An **acceptable use policy (AUP)** outlines what the organization considers to be the appropriate use of company resources, such as computer systems, e-mail, Internet access, and networks. Organizations should be concerned about personal use of organizational assets that does not benefit the company.

The goal of the AUP is to ensure employee productivity while limiting organizational liability through inappropriate use of the organization's assets. The AUP should clearly delineate what activities are not allowed. It should address issues such as the use of resources to conduct personal business, installation of hardware or software, remote access to systems and networks, the copying of company-owned software, and the responsibility of users to protect company assets, including data, software, and hardware. Statements regarding possible penalties for ignoring any of the policies (such as termination) should also be included.

Related to appropriate use of the organization's computer systems and networks by employees is the appropriate use by the organization. The most important of such issues is whether the organization considers it appropriate to monitor the employees' use of the systems and network.

If monitoring is considered appropriate, the organization should include a statement to this effect in the banner that appears at login. This repeatedly warns employees, and possible intruders, that their actions are subject to monitoring and that any misuse of the system will not be tolerated. Should the organization need to use in a civil or criminal case any information gathered during monitoring, the issue of whether the employee had an expectation of privacy, or whether it was even legal for the organization to be monitoring, is simplified if the organization can point to a statement that is always displayed that instructs users that use of the system constitutes consent to monitoring. Before any monitoring is conducted, or the actual wording on the warning message is created, the organization's legal counsel should be consulted to determine the appropriate way to address this issue in the particular jurisdiction.

In today's highly connected environment, every organization should have an AUP that spells out to all employees what the organization considers appropriate and inappropriate use of its computing and networks resources. Having this policy may be critical should the organization need to take disciplinary actions based on an abuse of its resources.

Internet Usage Policy

In today's highly connected environment, employee use of access to the Internet is of particular concern. The goal of the *Internet usage policy* is to ensure maximum employee productivity and to limit potential liability to the organization from inappropriate use of the Internet in a workplace. The Internet provides a tremendous temptation for employees to waste hours as they surf the Web for the scores of games from the previous night, conduct quick online stock transactions, or read the review of the latest blockbuster movie everyone is talking about. In addition, allowing employees to visit sites that may be considered offensive to others (such as pornographic or hate sites) can open the company to accusations of condoning a hostile work environment and result in legal liability.

The Internet usage policy needs to address what sites employees are allowed to visit and what sites they are not allowed to visit. If the company allows them to surf the Web during nonwork hours, the policy needs to clearly spell out the acceptable parameters, in terms of when they are allowed to do this and what sites they are still prohibited from visiting (such as potentially offensive sites). The policy should also describe under what circumstances an employee would be allowed to post something from the organization's network on the Web (on a blog, for example). A necessary addition to this policy would be the procedure for an employee to follow to obtain permission to post the object or message.

E-Mail Usage Policy

Related to the Internet usage policy is the *e-mail usage policy*, which deals with what the company will allow employees to send in, or as attachments to, e-mail messages. This policy should spell out whether nonwork e-mail traffic is allowed at all or is at least severely restricted. It needs to cover the type of message that would be considered inappropriate to send to other employees (for example, no offensive language, no sex-related or ethnic jokes, no harassment, and so on). The policy should also specify any disclaimers that must be attached to an employee's message sent to an individual outside the company. The policy should remind employees of the risks of clicking on links in e-mails, or opening attachments, as these can be social engineering attacks.

Clean Desk Policy

Preventing access to information is also important in the work area. Firms with sensitive information should have a "clean desk policy" specifying that sensitive information must not be left unsecured in the work area when the worker is not present to act as custodian. Even leaving the desk area and going to the bathroom can leave information exposed and subject to compromise. The clean desk policy should identify and prohibit things that are not obvious upon first glance, such as passwords on sticky notes under keyboards and mouse pads or in unsecured desk drawers. All of these elements that demonstrate the need for a clean desk are lost if employees do not make them personal. Training for clean desk activities needs to make the issue a personal one, where consequences are understood and the workplace reinforces the positive activity.

Bring Your Own Device (BYOD) Policy

Everyone seems to have a smartphone, a tablet, or other personal Internet device that they use in their personal lives. Bringing these to work is a natural extension of one's normal activities, but this raises the question of what policies are appropriate before a firm allows these devices to connect to the corporate network and access company data. Like all other policies, planning is needed to define the appropriate pathway to the company objectives. Personal devices offer cost savings and positive user acceptance, and in many cases these factors make allowing BYOD a sensible decision.

The primary purpose of a BYOD policy is to lower the risk associated with connecting a wide array of personal devices to a company's network and accessing sensitive data on them. This places security, in the form of risk management, as a center element of a BYOD policy. Devices need to be maintained in a current, up-to-date software posture, and with certain security features, such as screen locks and passwords enabled. Remote wipe and other features should be enabled, and highly sensitive data, especially in aggregate, should not be allowed on the devices. Users should have specific training as to what is allowed and what isn't and should be made aware of the increased responsibility associated with a mobile means of accessing corporate resources.

In some cases it may be necessary to define a policy associated with personally owned devices. This policy will describe the rules and regulations associated with use of personally owned devices with respect to corporate data, network connectivity, and security risks.

Privacy Policy

Customers place an enormous amount of trust in organizations to which they provide personal information. These customers expect their information to be kept secure so that unauthorized individuals will not gain access to it and so that authorized users will not use the information in unintended ways. Organizations should have a *privacy policy* that explains what their guiding principles will be in guarding personal data to which they are given access.

A special category of private information that is becoming increasingly important today is personally identifiable information (PII). This category of information includes any data that can be used to uniquely identify an individual. This would include an individual's name, address, driver's license number, and other details. An organization that collects PII on its employees and customers must make sure that it takes all necessary measures to protect the data from compromise.

Cross Check

Privacy

Privacy is an important consideration in today's computing environment. As such, it has been given its own chapter, Chapter 25. Additional details on privacy issues can be found there.

Due Care and Due Diligence

Due care and due diligence are terms used in the legal and business community to define reasonable behavior. Basically, the law recognizes the responsibility of an individual or organization to act reasonably relative to another party. If party A alleges that the actions of party B have caused it loss or injury, party A must prove that party B failed to exercise due care or due diligence and that this failure resulted in the loss or injury. These terms often are used synonymously, but **due care** generally refers to the standard of care a reasonable person is expected to exercise in all situations, whereas **due diligence** generally refers to the standard of care a business is expected to exercise in preparation for a business transaction. An organization must take reasonable precautions before entering a business transaction or it might be found to have acted irresponsibly. In terms of security, organizations are expected to take reasonable precautions to protect the information that they maintain on individuals. Should a person suffer a loss as a result of negligence on the part of an organization in terms of its security, that person typically can bring a legal suit against the organization.

The standard applied—reasonableness—is extremely subjective and often is determined by a jury. The organization will need to show that it had taken reasonable precautions to protect the information, and that, despite these precautions, an unforeseen security event occurred that caused the injury to the other party. Since this is so subjective, it is hard to describe what would be considered reasonable, but many sectors have a set of "security best practices" for their industry, which provides a basis for organizations in that sector to start from. If the organization decides not to follow any of the best practices accepted by the industry, it needs to be prepared to justify its reasons in court should an incident occur. If the sector the organization is in has regulatory requirements, justifying why the mandated security practices were not followed will be much more difficult (if not impossible).

Tech Tip

Prudent Person Principle

The concepts of due care and due diligence are connected. Due care addresses whether the organization has a minimal set of policies that provides reasonable assurance of success in maintaining security. Due diligence requires that management actually do something to ensure security, such as implement procedures for testing and review of audit records, internal security controls, and personnel behavior. The standard applied is one of a "prudent person"; would a prudent person find the actions appropriate and sincere? To apply this standard, all one has to do is ask the following question for the issue under consideration: "What would a prudent person do to protect and ensure that the security features and procedures are working or adequate?" Failure of a security feature or procedure doesn't necessarily mean the person acted imprudently.

Due diligence is the application of a specific standard of care. *Due care* is the degree of care that an ordinary person would exercise.

Due Process

Due process is concerned with guaranteeing fundamental fairness, justice, and liberty in relation to an individual's legal rights. In the United States, due process is concerned with the guarantee of an individual's rights as outlined by the Constitution and Bill of Rights. Procedural due process is based on the concept of what is "fair." Also of interest is the recognition by courts of a series of rights that are not explicitly specified by the Constitution but that the courts have decided are implicit in the concepts embodied by the Constitution. An example of this is an individual's right to privacy. From an organization's point of view, due process may come into play during an administrative action that adversely affects an employee. Before an employee is terminated, for example, were all of the employee's rights protected? An actual example pertains to the rights of privacy regarding employees' e-mail messages. As the number of cases involving employers examining employee e-mails grows, case law continues to be established and the courts eventually will settle on what rights an employee can expect. The best thing an employer can do if faced with this sort of situation is to work closely with HR staff to ensure that appropriate policies are followed and that those policies are in keeping with current laws and regulations.

Incident Response Policies and Procedures

No matter how careful an organization is, eventually a security incident of some sort will occur. When it happens, how effectively the organization responds to it will depend greatly on how prepared it is to handle incidents. An **incident response policy** and associated procedures should be developed to outline how the organization will prepare for security incidents and respond to them when they occur. Waiting until an incident happens is not the right time to establish your policies—they need to be designed in advance. The incident response policy should cover five phases: preparation, detection, containment and eradication, recovery, and follow-up actions.

Cross Check

Incident Response

Incident response is covered in detail in Chapter 22. This section serves only as an introduction to policy elements associated with the topic. For complete details on incident response, please examine Chapter 22.

Security Awareness and Training

Security awareness and training programs can enhance an organization's security posture in two direct ways. First, they teach personnel how to follow the correct set of actions to perform their duties in a secure manner. Second, they make personnel aware of the indicators and effects of social engineering attacks.

There are many tasks that employees perform that can have information security ramifications. Properly trained employees are able to perform their duties in a more effective manner, including their duties associated with information security. The extent of information security training will vary depending on the organization's environment and the level of threat, but initial employee security training at the time of being hired is important, as is periodic refresher training. A strong security education and awareness training program can go a long way toward reducing the chance that a social engineering attack will be successful. Security awareness programs and campaigns, which might include seminars, videos, posters, newsletters, and similar materials, are also fairly easy to implement and are not very costly.

Security Policy Training and Procedures

Personnel cannot be expected to perform complex tasks without training with respect to the tasks and expectations. This applies both to the security policy and to operational security details. If employees are going to be expected to comply with the organization's security policy, they must be properly trained in its purpose, meaning, and objectives. Training with respect to the information security policy, individual responsibilities, and expectations is something that requires periodic reinforcement through refresher training.

Because the security policy is a high-level directive that sets the overall support and executive direction with respect to security, it is important that the meaning of this message be translated and supported. Second-level policies such as password, access, information handling, and acceptable use policies also need to be covered. The collection of policies should paint a picture describing the desired security culture of the organization. The training should be designed to ensure that people see and understand the whole picture, not just the elements.

Role-based Training

For training to be effective, it needs to be targeted to the user with regard to their role in the subject of the training. While all employees may need general security awareness training, they also need specific training in areas where they have individual responsibilities. Role-based training with regard to information security responsibilities is an important part of information security training.

If a person has job responsibilities that may impact information security, then role-specific training is needed to ensure that the individual understands the responsibilities as they relate to information security. Some roles, such as system administrator or developer, have clearly defined information security responsibilities. The roles of others, such as project manager or purchasing manager, have information security impacts that are less obvious, but these roles require training as well. In fact, the less-obvious but wider-impact roles of middle management can have a large effect on the information security culture, and thus if a specific outcome is desired, it requires training.

As in all personnel-related training, two elements need attention. First, retraining over time is necessary to ensure that personnel keep proper levels of knowledge. Second, as people change jobs, a reassessment of the

required training basis is needed, and additional training may be required. Maintaining accurate training records of personnel is the only way this can be managed in any significant enterprise.

Compliance with Laws, Best Practices, and Standards

There is a wide array of laws, regulations, contractual requirements, standards, and best practices associated with information security. Each places its own set of requirements upon an organization and its personnel. The only effective way for an organization to address these requirements is to build them into their own policies and procedures. Training to one's own policies and procedures would then translate into coverage of these external requirements.

It is important to note that many of these external requirements impart a specific training and awareness component upon the organization. Organizations subject to the requirements of the Payment Card Industry Data Security Standard (PCI DSS), Gramm Leach Bliley Act (GLBA), or Health Insurance Portability Accountability Act (HIPAA) are among the many that must maintain a specific information security training program. Other organizations should do so as a matter of best practice.

User Habits

Individual user responsibilities vary between organizations and the type of business each organization is involved in, but there are certain very basic responsibilities that all users should be instructed to adopt:

- Lock the door to your office or workspace, including drawers and cabinets.
- Do not leave sensitive information inside your car unprotected.
- Secure storage media containing sensitive information in a secure storage device.
- Shred paper containing organizational information before discarding it.
- Do not divulge sensitive information to individuals (including other employees) who do not have an authorized need to know it.
- Do not discuss sensitive information with family members. (The most common violation of this rule occurs in regard to HR information, as employees, especially supervisors, may complain to their spouse or friends about other employees or about problems that are occurring at work.)
- Protect laptops and other mobile devices that contain sensitive or important organization information wherever the device may be stored or left. (It's a good idea to ensure that sensitive information is encrypted on the laptop or mobile device so that, should the equipment be lost or stolen, the information remains safe.)
- Be aware of who is around you when discussing sensitive corporate information. Does everybody within earshot have the need to hear this information?

- Enforce corporate access control procedures. Be alert to, and do not allow, piggybacking, shoulder surfing, or access without the proper credentials.
- Be aware of the correct procedures to report suspected or actual violations of security policies.
- Follow procedures established to enforce good password security practices. Passwords are such a critical element that they are frequently the ultimate target of a social engineering attack. Though such password procedures may seem too oppressive or strict, they are often the best line of defense.
- **User habits** are a front-line security tool in engaging the workforce to improve the overall security posture of an organization.

User responsibilities are easy training topics about which to ask questions on the CompTIA Security+ exam, so commit to memory your knowledge of the points listed here.

New Threats and Security Trends/Alerts

At the end of the day, information security practices are about managing risk, and it is well known that the risk environment is one marked by constant change. The ever-evolving threat environment frequently encounters new threats, new security issues, and new forms of defense. Training people to recognize the new threats necessitates continual awareness and training refresher events.

New Viruses

New forms of viruses, or malware, are being created every day. Some of these new forms can be highly destructive and costly, and it is incumbent upon all users to be on the lookout for and take actions to avoid exposure. Poor user practices are counted on by malware authors to assist in the spread of their attacks. One way of explaining proper actions to users is to use an analogy to cleanliness. Training users to practice good hygiene in their actions can go a long way toward assisting the enterprise in defending against these attack vectors.

Phishing Attacks

The best defense against phishing and other social engineering attacks is an educated and aware body of employees. Continual refresher training about the topic of social engineering and specifics about current attack trends are needed to keep employees aware of and prepared for new trends in social engineering attacks. Attackers rely upon an uneducated, complacent, or distracted workforce to enable their attack vector. Social engineering has become the gateway for many of the most damaging attacks in play today. Social engineering is covered extensively in Chapter 4.

Social Networking and P2P

With the rise in popularity of peer-to-peer (P2P) communications and social networking sites—notably Facebook, Twitter, and LinkedIn—many people have gotten into a habit of sharing too much information. Using a status of "Returning from sales call to XYZ company" reveals information to people who have no need to know this information. Confusing sharing with

friends and sharing business information with those who don't need to know is a line people are crossing on a regular basis. Don't be the employee who mixes business and personal information and releases information to parties who should not have it, regardless of how innocuous it may seem.

Users need to understand the importance of not using common programs such as torrents and other file sharing in the workplace, as these programs can result in infection mechanisms and data-loss channels. The information security training and awareness program should cover these issues. If the issues are properly explained to employees, their motivation to comply won't simply be to avoid adverse personnel action for violating a policy; they will want to assist in the security of the organization and its mission.

Training Metrics and Compliance

Training and awareness programs can yield much in the way of an educated and knowledgeable workforce. Many laws, regulations, and best practices have requirements for maintaining a trained workforce. Having a record-keeping system to measure compliance with attendance and to measure the effectiveness of the training is a normal requirement. Simply conducting training is not sufficient. Following up and gathering training metrics to validate compliance and security posture is an important aspect of security training management.

A number of factors deserve attention when managing security training. Because of the diverse nature of role-based requirements, maintaining an active, up-to-date listing of individual training and retraining requirements is one challenge. Monitoring the effectiveness of the training is yet another challenge. Creating an effective training and awareness program when measured by actual impact on employee behavior is a challenging endeavor. Training needs to be current, relevant, and interesting to engage employee attention. Simple repetition of the same training material has not proven to be effective, so regularly updating the program is a requirement if it is to remain effective over time.

Tech Tip

Security Training Records

Requirements for both periodic training and retraining drive the need for good training records. Maintaining proper information security training records is a requirement of several laws and regulations and should be considered a best practice.

Interoperability Agreements

Many business operations involve actions between many different parties—some within an organization, and some in different organizations. These actions require communication between the parties, defining the responsibilities and expectations of the parties, the business objectives, and the environment within which the objectives will be pursued. To ensure an agreement is understood between the parties, written agreements are used. Numerous forms of legal agreements and contracts are used in business, but with respect to security, some of the most common ones are the service level agreement, business partnership agreement, memorandum of understanding, and interconnection security agreement.

Service Level Agreements

Service level agreements (SLAs) are contractual agreements between entities that describe specified levels of service that the servicing entity agrees to guarantee for the customer. SLAs essentially set the requisite level of performance of a given contractual service. SLAs are typically included as part of a service contract and set the level of technical expectations. An SLA can define specific services, the performance level associated with a service, issue management and resolution, and so on. SLAs are negotiated between customer and supplier and represent the agreed-upon terms. An organization contracting with a service provider should remember to include in the agreement a section describing the service provider's responsibility in terms of business continuity and disaster recovery. The provider's backup plans and processes for restoring lost data should also be clearly described.

Typically, a good SLA will satisfy two simple rules. First, it will describe the entire set of product or service functions in sufficient detail that their requirement will be unambiguous. Second, the SLA will provide a clear means of determining whether a specified function or service has been provided at the agreed-upon level of performance.

Business Partnership Agreement

A **business partnership agreement (BPA)** is a legal agreement between partners establishing the terms, conditions, and expectations of the relationship between the partners. These details can cover a wide range of issues, including typical items such as the sharing of profits and losses, the responsibilities of each partner, the addition or removal of partners, and any other issues. The Uniform Partnership Act (UPA), established by state law and convention, lays out a uniform set of rules associated with partnerships to resolve any partnership terms. The terms in a UPA are designed as "one size fits all" and are not typically in the best interest of any specific partnership. To avoid undesired outcomes that may result from UPA terms, it is best for partnerships to spell out specifics in a BPA.

Memorandum of Understanding

A **memorandum of understanding (MOU)** is a legal document used to describe a bilateral agreement between parties. It is a written agreement expressing a set of intended actions between the parties with respect to some common pursuit or goal. It is more formal and detailed than a simple handshake, but it generally lacks the binding powers of a contract. It is also common to find MOUs between different units within an organization to detail expectations associated with the common business interest.

Interconnection Security Agreement

An **interconnection security agreement (ISA)** is a specialized agreement between organizations that have interconnected IT systems, the purpose of which is to document the security requirements associated with the interconnection. An ISA can be a part of an MOU detailing the specific technical security aspects of a data interconnection.

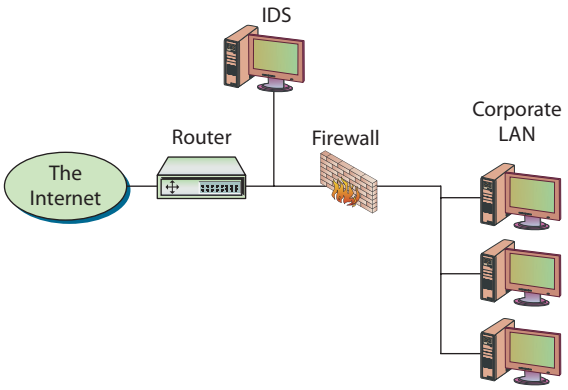
Be sure you understand the differences between the interoperability agreements SLA, BPA, MOU, and ISA. The differences hinge upon the purpose for each document.

The security perimeter, with its several layers of security, along with additional security mechanisms that may be implemented on each system (such as user IDs/passwords), creates what is sometimes known as *defense-in-depth.* This implies that security is enhanced when there are multiple layers of security (the depth) through which an attacker would have to penetrate to reach the desired goal.

The Security Perimeter

The discussion to this point has not included any mention of the specific technology used to enforce operational and organizational security or a description of the various components that constitute the organization's security perimeter. If the average administrator were asked to draw a diagram depicting the various components of their network, the diagram would probably look something like Figure 3.1.

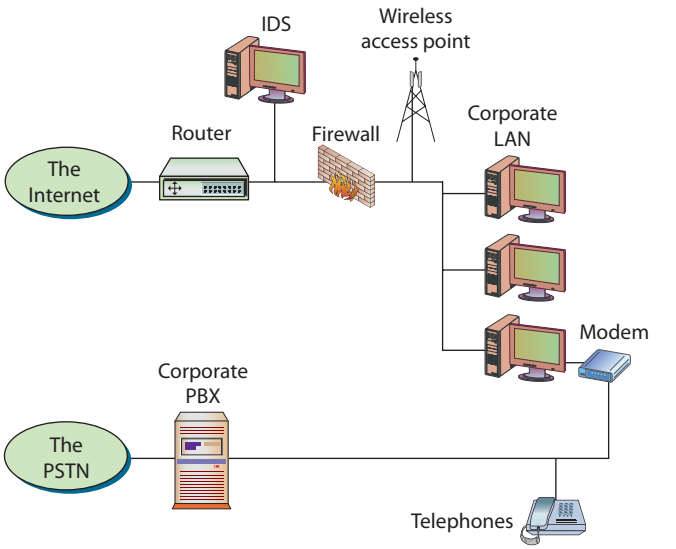
This diagram includes the major components typically found in a network. The connection to the Internet generally has some sort of protection attached to it such as a firewall. An intrusion detection system (IDS), also often part of the security perimeter for the organization, may be either on the inside or the outside of the firewall, or it may in fact be on both sides. The specific location depends on the company and what it is more concerned about preventing (that is, insider threats or external threats). The router can also be thought of as a security device, as it can be used to enhance security such as in the case of wireless routers that can be used to enforce encryption settings. Beyond this security perimeter is the corporate network. Figure 3.1 is obviously a very simple depiction—an actual network can have numerous subnets and extranets as well as wireless access points—but the basic components are present. Unfortunately, if this were the diagram provided by the administrator to show the organization's basic network structure, the administrator would have missed a very important component. A more astute administrator would provide a diagram more like Figure 3.2.



• **Figure 3.1** Basic diagram of an organization's network

This diagram includes other possible access points into the network, including the public switched telephone network (PSTN) and wireless access points. The organization may or may not have any authorized modems or wireless networks, but the savvy administrator would realize that the potential exists for unauthorized versions of both.

When considering the policies, procedures, and guidelines needed to implement security for the organization, both networks need to be considered. Another development that has brought the telephone and computer networks together is the implementation of *voice over IP (VoIP),* which eliminates the traditional land lines in an organization and replaces them with special telephones that connect to the IP data network.



• **Figure 3.2** A more complete diagram of an organization's network

While Figure 3.2 provides a more comprehensive view of the various components that need to be protected, it is still incomplete. Most experts will agree that the biggest danger to any organization does not come from external attacks but rather from the insider—a disgruntled employee or somebody else who has physical access to the facility. Given physical access to an office, the knowledgeable attacker will quickly find the information needed to gain access to the organization's computer systems

and network. Consequently, every organization also needs security policies, procedures, and guidelines that cover physical security, and every security administrator should be concerned with these as well. While physical security (which can include such things as locks, cameras, guards and entry points, alarm systems, and physical barriers) will probably not fall under the purview of the security administrator, the operational state of the organization's physical security measures is just as important as many of the other network-centric measures.

An increasing number of organizations are implementing VoIP solutions to bring the telephone and computer networks together. While there are some tremendous advantages to doing this in terms of both increased capabilities and potential monetary savings, bringing the two networks together may also introduce additional security concerns. Another common method to access organizational networks today is through wireless access points. These may be provided by the organization itself to enhance productivity, or they may be attached to the network by users without organizational approval. The impact of all of these additional methods that can be used to access a network is to increase the complexity of the security problem.

Physical Security

Physical security consists of all mechanisms used to ensure that physical access to the computer systems and networks is restricted to only authorized users. Additional physical security mechanisms may be used to provide increased security for especially sensitive systems such as servers and devices such as routers, firewalls, and intrusion detection systems. When considering physical security, access from all six sides should be considered—not only should the security of obvious points of entry be examined, such as doors and windows, but the walls themselves as well as the floor and ceiling should also be considered. Questions such as the following should be addressed:

- Is there a false ceiling with tiles that can be easily removed?
- Do the walls extend to the actual ceiling or only to a false ceiling?
- Is there a raised floor?
- Do the walls extend to the actual floor, or do they stop at a raised floor?
- How are important systems situated?
- Do the monitors face away from windows, or could the activity of somebody at a system be monitored?
- Who has access to the facility?
- What type of access control is there, and are there any guards?
- Who is allowed unsupervised access to the facility?
- Is there an alarm system or security camera that covers the area?
- What procedures govern the monitoring of the alarm system or security camera and the response should unauthorized activity be detected?

These are just some of the numerous questions that need to be asked when examining the physical security surrounding a system.

Tech Tip

Physical Security Is Also Important to Computer Security

Computer security professionals recognize that they cannot rely only on computer security mechanisms to keep their systems safe. Physical security must be maintained as well, because in many cases, if an attacker gains physical access, he can steal data and destroy the system.

Physical Access Controls

The purpose of physical access controls is the same as that of computer and network access controls—you want to restrict access to only those who are authorized to have it. Physical access is restricted by requiring the individual to somehow authenticate that they have the right or authority to have

the desired access. As in computer authentication, access in the physical world can be based on something the individual has, something they know, or something they are. Frequently, when dealing with the physical world, the terms "authentication" and "access control" are used interchangeably.

The most common physical access control device, which has been around in some form for centuries, is a lock. Combination locks represent an access control device that depends on something the individual knows (the combination). Locks with keys depend on something the individual has (the key). Each of these has certain advantages and disadvantages. Combinations don't require any extra hardware, but they must be remembered (which means individuals may write them down—a security vulnerability in itself) and are hard to control. Anybody who knows the combination may provide it to somebody else. Key locks are simple and easy to use, but the key may be lost, which means another key has to be made or the lock has to be rekeyed. Keys may also be copied, and their dissemination can be hard to control. Newer locks replace the traditional key with a card that must be passed through a reader or placed against it. The individual may also have to provide a personal access code, thus making this form of access both a something-you-know and something-you-have method.

In addition to locks on doors, other common physical security devices include video surveillance and even simple access control logs (sign-in logs). While sign-in logs don't provide an actual barrier, they do provide a record of access and, when used in conjunction with a guard who verifies an individual's identity, can dissuade potential adversaries from attempting to gain access to a facility. As mentioned, another common access control mechanism is a human security guard. Many organizations employ a guard to provide an extra level of examination of individuals who want to gain access to a facility. Other devices are limited to their designed function. A human guard can apply common sense to situations that might have been unexpected. Having security guards also addresses the common practice of piggybacking (aka tailgating), where an individual follows another person closely to avoid having to go through the access control procedures.

Tech Tip

Physical and Information Security Convergence

In high-security sites, physical access controls and electronic access controls to information are interlocked. This means that before data can be accessed from a particular machine, the physical access control system must agree with the finding that the authorized party is present.

Biometrics

Access controls that utilize something you know (for example, combinations) or something you have (such as keys) are not the only methods to limit facility access to authorized individuals. A third approach is to utilize something unique about the individual—their fingerprints, for example—to identify them. Unlike the other two methods, the something-you-are method, known as **biometrics**, does not rely on the individual to either remember something or to have something in their possession. Biometrics is a more sophisticated access control approach and can be more expensive. Biometrics also suffer from false positives and false negatives, making them less than 100 percent effective. For this reason they are frequently used in conjunction with another form of authentication. The advantage is the user always has them (cannot leave at home or share) and they tend to have better entropy than passwords. Other methods to accomplish biometrics include handwriting analysis, retinal scans, iris scans, voiceprints, hand geometry, and facial geometry.

There are many similarities between authentication and access controls in computers and in the physical world. Remember the three common techniques for verifying a person's identity and access privileges: something you know, something you have, and something about you.

Both access to computer systems and networks and physical access to restricted areas can be controlled with biometrics. However, biometric methods for controlling physical access are generally not the same as those employed for restricting access to computer systems and networks. Hand geometry, for example, requires a fairly large device. This can easily be placed outside of a door to control access to the room but would not be as convenient to control access to a computer system, since a reader would need to be placed with each computer or at least with groups of computers. In a mobile environment where laptops are being used, a device such as a hand geometry reader would be unrealistic.

Tech Tip

Biometric Devices

Once only seen in spy or science fiction movies, biometrics such as hand and fingerprint readers, eye-scanning technology, and voiceprint devices are now becoming more common in the real world. The accuracy of these devices has improved and the costs have dropped, making them realistic solutions to many access control situations.

Physical Barriers

An even more common security feature than locks is a physical barrier. Physical barriers help implement the physical-world equivalent of layered security. The outermost layer of physical security should contain the more publicly visible activities. A guard at a gate in a fence, for example, would be visible by all who happen to pass by. As you progress through the layers, the barriers and security mechanisms should become less publicly visible to make determining what mechanisms are in place more difficult for observers. Signs are also an important element in security, as they announce to the public which areas are public and which are private. A *man trap* can also be used in this layered approach. It generally consists of a small space that is large enough for only one person at a time, with two locking doors. An individual has to enter the first door, close the first door, then attempt to open the second door. If unsuccessful, perhaps because they do not have the proper access code, the person can be caught inside this small location until security personnel show up.

Tech Tip

Signs

Signs can be an effective control, warning unauthorized personnel not to enter, locating critical elements for first responders, and providing paths to exits in emergencies. Proper signage is an important aspect of physical security controls.

In addition to walls and fences, open space can also serve as a barrier. While this may at first seem to be an odd statement, consider the use of large areas of open space around a facility. For an intruder to cross this open space takes time—time in which they are vulnerable and their presence may be discovered. In today's environment in which terrorist attacks have become more common, additional precautions should be taken for areas that may be considered a possible target for terrorist activity. In addition to open space, which is necessary to lessen the effect of explosions, concrete barriers that stop vehicles from getting too close to facilities should also be used. It is not necessary for these to be unsightly concrete walls; many facilities have placed large, round concrete circles, filled them with dirt, and then planted flowers and other plants to construct a large, immovable planter.

Environmental Issues

Environmental issues may not at first seem to be related to security, but when considering the availability of a computer system or network, they must be taken into consideration. Environmental issues include items such as **heating, ventilation, and air conditioning (HVAC)** systems, electrical power, and the "environments of nature." HVAC systems are used to maintain the

HVAC systems for server rooms and network equipment closets are important because the dense equipment environment can generate significant amounts of heat. HVAC outages can result in temperatures that are outside equipment operating ranges, forcing shutdowns.

comfort of an office environment. A few years back, they were also critical for the smooth operation of computer systems that had low tolerances for humidity and heat. Today's desktop systems are much more tolerant, and the limiting factor is now often the human user. The exception to this HVAC limitation is when large quantities of equipment are co-located, in server rooms and network equipment closets. In these heat-dense areas, HVAC is needed to keep equipment temperatures within reasonable ranges. Often certain security devices such as firewalls and intrusion detection systems are located in these same equipment closets and the loss of HVAC systems can cause these critical systems to fail. One interesting aspect of HVAC systems is that they themselves are often computer controlled and frequently provide remote access via telephone or network connections. These connections should be protected in a similar manner to computer modems, or else attackers may locate them and change the HVAC settings for an office or building.

Electrical power is obviously an essential requirement for computer systems and networks. Electrical power is subject to momentary surges and disruption. Surge protectors are needed to protect sensitive electronic equipment from fluctuations in voltage. An **uninterruptible power supply (UPS)** should be considered for critical systems so that a loss of power will not halt processing. The size of the batteries associated with a UPS will determine the amount of time that it can operate before it too loses power. Many sites ensure sufficient power to provide administrators the opportunity to cleanly bring the system or network down. For installations that require continuous operations, even in the event of a power outage, electric generators that automatically start when a loss of power is detected can be installed. These systems may take a few seconds to start before they reach full operation, so a UPS should also be considered to smooth the transition between normal and backup power.

Fire Suppression

Fires are a common disaster that can affect organizations and their computing equipment. Fire detection and fire suppression devices are two approaches to addressing this threat. Detectors can be useful because some may be able to detect a fire in its very early stages before a fire suppression system is activated, and they can potentially sound a warning. This warning could provide employees with the opportunity to deal with the fire before it becomes serious enough for the fire suppression equipment to kick in. Suppression systems come in several varieties, including sprinkler-based systems and gas-based systems. Standard sprinkler-based systems are not optimal for data centers because water will ruin large electrical infrastructures and most integrated circuit–based devices—such as computers. Gas-based systems are a good alternative, though they also carry special concerns. More extensive coverage of fire detection and suppression is provided in Chapter 8.

Wireless

When someone talks about wireless communication, they generally are referring to cellular telephones ("cell phones"). These devices have become ubiquitous in today's modern office environment. A cell phone network consists of the phones themselves, the cells with their accompanying base stations that they are used in, and the hardware and software that allow them to communicate. The base stations are made up of antennas, receivers, transmitters, and amplifiers. The base stations communicate with those cell phones that are currently in the geographical area that is serviced by that station. As a person travels across town, they may exit and enter multiple cells. The stations must conduct a handoff to ensure continuous operation for the cell phone. As the individual moves toward the edge of a cell, a mobile switching center notices the power of the signal beginning to drop, checks whether another cell has a stronger signal for the phone (cells frequently overlap), and, if so, switches operation to this new cell and base station. All of this is done without the user ever knowing that they have moved from one cell to another.

Wireless technology can also be used for networking. There are two main standards for wireless network technology. **Bluetooth** is designed as a short-range (approximately ten meters) personal area network (PAN) cable-replacement technology that can be built into a variety of devices, such as mobile phones, tablets, and laptop computers. The idea is to create low-cost wireless technology so that many different devices can communicate with each other. Bluetooth is also interesting because, unlike other wireless technology, it is designed so that devices can talk directly with each other without having to go through a central device (such as the base station described previously). This is known as *peer-to-peer communication.*

The other major wireless standard is the **IEEE 802.11** set of standards, which is well suited for the local area network (LAN) environment. 802.11 networks can operate either in an ad hoc peer-to-peer fashion or in infrastructure mode, which is more common. In infrastructure mode, computers with 802.11 network cards communicate with a wireless access point. This access point connects to the network so that the computers communicating with it are essentially also connected to the network.

While wireless networks are very useful in today's modern office (and home), they are not without their security problems. Access points are generally placed throughout a building so that all employees can access the corporate network. The transmission and reception areas covered by access points are not easily controlled. Consequently, many publicly accessible areas might fall into the range of one of the organization's access points, or its Bluetooth-enabled systems, and thus the corporate network may become vulnerable to attack. Wireless networks are designed to incorporate some security measures, but all too often the networks are set up without security enabled, and serious security flaws exist in the 802.11 design.

Tech Tip

Wireless Network Security Issues

Due to a number of advantages, such as the ability to take your laptop with you as you move around your building and still stay connected, wireless networks have grown in popularity. They also eliminate the need to string network cables all over the office. At the same time, however, they can be a security nightmare if not adequately protected. The signal for your network doesn't stop at your office door or wall just because it is there. It will continue propagating to areas that may be open to anybody. This provides the opportunity for others to access your network. To avoid this, you must take steps such as encrypting transmissions so that your wireless network doesn't become the weak link in your security chain.

Cross Check

Wireless Networks

Wireless network security is discussed in this chapter in relationship to physical issues such as the placement of wireless access points. There are, however, numerous other issues with wireless security, which are discussed in Chapter 12. Make sure to understand how the physical location of wireless access points affects the other wireless security issues.

Electromagnetic Eavesdropping

In 1985, a paper by Wim van Eck of the Netherlands described what became known as the van Eck phenomenon. In the paper van Eck described how eavesdropping on what was being displayed on monitors could be accomplished by picking up and then decoding the electromagnetic interference produced by the monitors. With the appropriate equipment, the exact image of what is being displayed can be re-created some distance away. While the original paper discussed emanations as they applied to video display units (monitors), the same phenomenon applies to other devices such as printers and computers.

This phenomenon had actually been known about for quite some time before van Eck published his paper. The U.S. Department of Defense used the term **TEMPEST** (referred to by some as the *Transient ElectroMagnetic Pulse Emanation STandard*) to describe both a program in the military to control these electronic emanations from electrical equipment and the actual process for controlling the emanations. There are three basic ways to prevent these emanations from being picked up by an attacker:

- Put the equipment beyond the point that the emanations can be picked up.
- Provide shielding for the equipment itself.
- Provide a shielded enclosure (such as a room) to put the equipment in.

One of the simplest ways to protect against equipment being monitored in this fashion is to put enough distance between the target and the attacker. The emanations can be picked up from only a limited distance. If the physical security for the facility is sufficient to put enough space between the equipment and publicly accessible areas that the signals cannot be picked up, then the organization doesn't have to take any additional measures to ensure security.

Distance is not the only way to protect against eavesdropping on electronic emanations. Devices can be shielded so their emanations are blocked. Acquiring enough property to provide the necessary distance needed to protect against an eavesdropper may be possible if the facility is in the country with lots of available land surrounding it. Indeed, for smaller organizations that occupy only a few offices or floors in a large office building, it would

be impossible to acquire enough space. In this case, the organization may resort to purchasing shielded equipment. A "TEMPEST approved" computer will cost significantly more than what a normal computer would cost. Shielding a room (in what is known as a *Faraday cage*) is also an extremely expensive endeavor.

A natural question to ask is, how prevalent is this form of attack? The equipment needed to perform electromagnetic eavesdropping is not readily available, but it would not cost an inordinate amount of money to produce it. The cost could certainly be afforded by any large corporation, and industrial espionage using such a device is a possibility. While there are no public records of this sort of activity being conducted, it is reasonable to assume that it does take place in large corporations and the government, especially in foreign countries.

One of the challenges in security is determining how much to spend on security without spending too much. Security spending should be based on likely threats to your systems and network. While electronic emanations can be monitored, the likelihood of this taking place in most situations is remote, which makes spending on items to protect against it at best a low priority.

Modern Eavesdropping

Not just electromagnetic information can be used to carry information out of a system to an adversary. Recent advances have demonstrated the feasibility of using the webcams and microphones on systems to spy on users, recording keystrokes and other activities. There are even devices built to intercept the wireless signals between wireless keyboards and mice and transmit them over another channel to an adversary. USB-based keyloggers can be placed in the back of machines, as in many cases the back of a machine is unguarded or facing the public (watch for this the next time you see a receptionist's machine).

Chapter 3 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following regarding operational and organizational security.

Identify various operational aspects to security in your organization

- Prevention technologies are designed to keep individuals from being able to gain access to systems or data they are not authorized to use.
- Previously in operational environments, prevention was extremely difficult and relying on prevention technologies alone was not sufficient. This led to the rise of technologies to detect and respond to events that occur when prevention fails.
- An important part of any organization's approach to implementing security is to establish policies, procedures, standards, and guidelines to detail what users and administrators should be doing to maintain the security of the systems and network.

Identify various policies and procedures in your organization

- Policies, procedures, standards, and guidelines are important in establishing a security program within an organization.
- The security policy and supporting policies play an important role in establishing and managing system risk.
- Policies and procedures associated with Human Resources functionality include job rotation, mandatory vacations, and hiring and termination policies.

Identify the security awareness and training needs of an organization

- Security training and awareness efforts are vital in engaging the workforce to act within the desired range of conduct with respect to security.
- Security awareness and training is important in achieving compliance objectives.
- Security awareness and training should be measured and managed as part of a comprehensive security program.

Understand the different types of agreements employed in negotiating security requirements

- The different interoperability agreements, including SLA, BPA, MOU and ISA, are used to establish security expectations between various parties.

Describe the physical security components that can protect your computers and network

- Physical security consists of all mechanisms used to ensure that physical access to the computer systems and networks is restricted to only authorized users.
- The purpose of physical access controls is the same as that of computer and network access controls—to restrict access to only those who are authorized to have it.
- The careful placement of equipment can provide security for known security problems exhibited by wireless devices and that arise due to electronic emanations.

Identify environmental factors that can affect security

- Environmental issues are important to security because they can affect the availability of a computer system or network.
- Loss of HVAC systems can lead to overheating problems that can affect electronic equipment, including security-related devices.
- The frequency of natural disasters is a contributing factor that must be considered when making contingency processing plans for an installation.
- Fires are a common problem for organizations. Two general approaches to addressing this problem are fire detection and fire suppression.

Identify factors that affect the security of the growing number of wireless technologies used for data transmission

- Wireless networks have many security issues, including the transmission and reception areas covered by access points, which are not easily controlled and can thus provide easy network access for intruders.

Prevent disclosure through electronic emanations

- With the appropriate equipment, the exact image of what is being displayed on a computer monitor can be re-created some distance away, allowing eavesdroppers to view what you are doing.
- Providing a lot of distance between the system you wish to protect and the closest place an eavesdropper could be is one way to protect against eavesdropping on electronic emanations. Devices can also be shielded so that their emanations are blocked.

Key Terms

acceptable use policy (AUP) *(50)*
biometrics *(62)*
Bluetooth *(65)*
business partnership agreement (BPA) *(59)*
due care *(53)*
due diligence *(53)*
guidelines *(43)*
heating, ventilation, and air conditioning (HVAC) *(63)*
IEEE 802.11 *(65)*
incident response policy *(54)*
interconnection security agreement (ISA) *(59)*
memorandum of understanding (MOU) *(59)*
physical security *(61)*
policies *(43)*
procedures *(43)*
security policy *(44)*
service level agreement (SLA) *(59)*
standards *(43)*
TEMPEST *(66)*
uninterruptible power supply (UPS) *(64)*
user habits *(57)*

Key Terms Quiz

Use terms from the Key Terms list to complete the sentences that follow. Don't use the same term more than once. Not all terms will be used.

1. _____ are high-level statements made by management that lay out the organization's position on some issue.
2. The collective term used to refer to the systems that are used to maintain the comfort of an office environment and that are often controlled by computer systems is _____.
3. A(n) _____ is a device designed to provide power to essential equipment for a period of time when normal power is lost.
4. _____ are a foundational security tool in engaging the workforce to improve the overall security posture of an organization.
5. _____ are accepted specifications providing specific details on how a policy is to be enforced.
6. _____ is a wireless technology designed as a short-range (approximately ten meters) personal area network (PAN) cable-replacement technology that may be built into a variety of devices such as mobile phones, tablets, and laptop computers.
7. A(n) _____ is a legal document used to describe a bilateral agreement between parties.
8. _____ are step-by-step instructions that describe exactly how employees are expected to act in a given situation or to accomplish a specific task.
9. The set of standards for wireless networks that is well suited for the LAN environment and whose normal mode is to have computers with network cards communicating with a wireless access point is _____.
10. A(n) _____ is a legal agreement between organizations establishing the terms, conditions, and expectations of the relationship between them.

Multiple-Choice Quiz

1. Which of the following is a physical security threat?
   - **A.** Cleaning crews are allowed unsupervised access because they have a contract.
   - **B.** Employees undergo background criminal checks before being hired.
   - **C.** All data is encrypted before being backed up.
   - **D.** All the above.
2. The benefit of fire detection equipment over fire suppression devices is:
   - **A.** Fire detection equipment is regulated, whereas fire suppression equipment is not.
   - **B.** Fire detection equipment will often catch fires at a much earlier stage, meaning that the fire can be addressed before significant damage can occur.
   - **C.** Fire detection equipment is much more reliable than fire suppression equipment.
   - **D.** There is no advantage of fire detection over fire suppression other than the cost of fire detection equipment is much less than the cost of fire suppression equipment.
3. Which of the following is a contractual agreement between entities that describes specified levels of service that the servicing entity agrees to guarantee for the customer?
   - **A.** Service level agreement
   - **B.** Support level agreement
   - **C.** Memorandum of understanding
   - **D.** Business service agreement
4. During which step of the policy lifecycle does training of users take place?
   - **A.** Plan for security.
   - **B.** Implement the plans.
   - **C.** Monitor the implementation.
   - **D.** Evaluate for effectiveness.
5. Biometric access controls are typically used in conjunction with another form of access control because:
   - **A.** Biometrics are still expensive.
   - **B.** Biometrics cannot be copied.
   - **C.** Biometrics are not always convenient to use.
   - **D.** Biometrics are not 100 percent accurate, having some level of misidentifications.
6. Procedures can be described as:
   - **A.** High-level, broad statements of what the organization wants to accomplish
   - **B.** Step-by-step instructions on how to implement the policies
   - **C.** Mandatory elements regarding the implementation of a policy
   - **D.** Recommendations relating to a policy
7. What technique can be used to protect against electromagnetic eavesdropping (known as the van Eck phenomenon)?
   - **A.** Provide sufficient distance between the potential target and the nearest location an attacker could be.
   - **B.** Put the equipment that you are trying to protect inside a shielded room.
   - **C.** Purchase "TEMPEST approved" equipment.
   - **D.** All of the above.
8. Key user habits that can improve security efforts include:
   - **A.** Do not discuss business issues outside of the office.
   - **B.** Never leave laptops or tablets inside your car unattended.
   - **C.** Be alert of people violating physical access rules (piggybacking through doors).
   - **D.** Items B and C.

9. When should a human security guard be used for physical access control?
   - **A.** When other electronic access control mechanisms will not be accepted by employees
   - **B.** When necessary to avoid issues such as piggybacking, which can occur with electronic access controls
   - **C.** When other access controls are too expensive to implement
   - **D.** When the organization wants to enhance its image

10. What device should be used by organizations to protect sensitive equipment from fluctuations in voltage?
   - **A.** A surge protector
   - **B.** An uninterruptible power supply
   - **C.** A backup power generator
   - **D.** A redundant array of inline batteries (RAIB)

Essay Quiz

1. Describe the difference between fire suppression and fire detection systems.
2. Discuss why physical security is also important to computer security professionals.
3. Why should we be concerned about HVAC systems when discussing security?
4. Outline the various components that make up (or should make up) an organization's security perimeter. Which of these can be found in your organization (or school)?

Lab Projects

• Lab Project 3.1

Take a tour of your building on campus or at work. What is secured at night when workers are absent? Record the location and type of physical access control devices. How do these access controls change at night when workers are absent? How well trained do guards and other employees appear to be? Do they allow "piggybacking" (somebody slipping into a facility behind an authorized individual without being challenged)? What are the policies for visitors and contractors? How does this all impact physical security?

• Lab Project 3.2

Describe the four steps of the policy lifecycle. Obtain a policy from your organization (such as an acceptable use policy or Internet usage policy). How are users informed of this policy? How often is it reviewed? How would changes to it be suggested and who would make decisions on whether the changes were accepted?