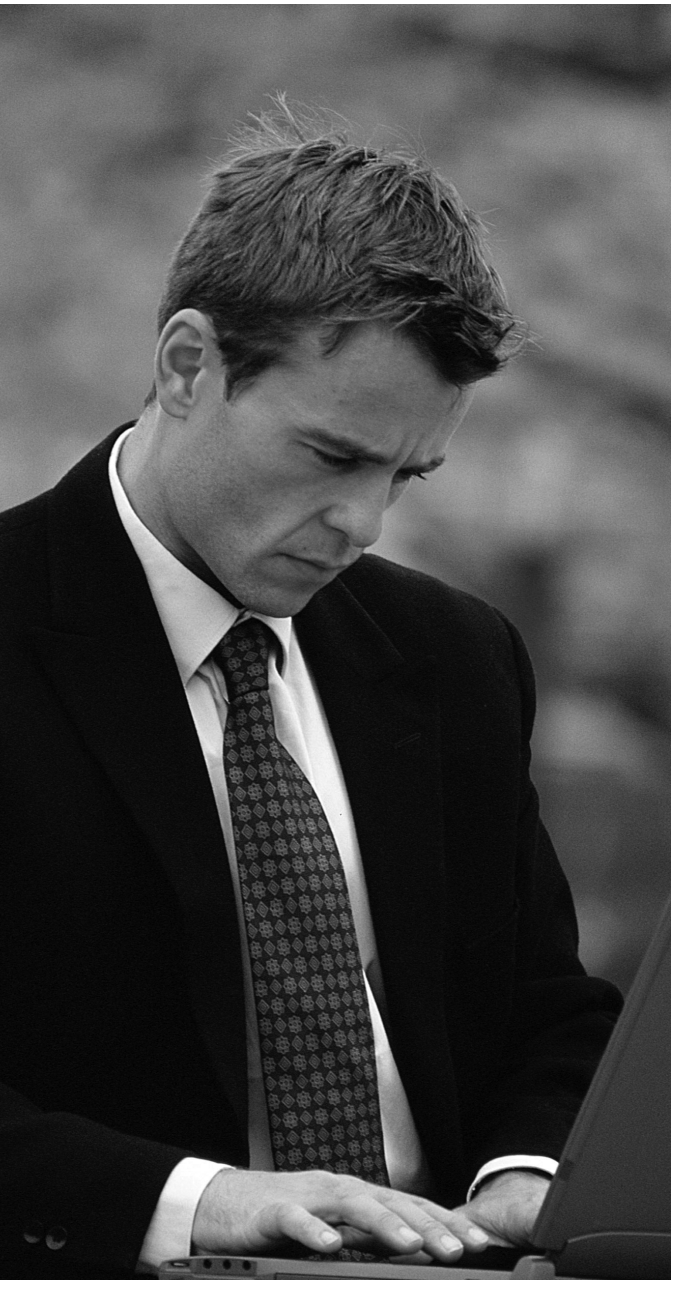

CHAPTER 5

POLICY, PERSONNEL, AND EQUIPMENT AS SECURITY ENABLERS

Enhanced security, as a field of business, is still relatively young. Security audit firms are burgeoning, swiftly heeding the call of urgency in many organizations. The auditing process can reveal many evils, not the least of which is an insufficient security policy framework. Given the threats that exist today, organizations would be well served with security policies that take the corporation's unique structure into account and create procedures that work to increase its business flexibility.

Making the business case for network security requires acute awareness of process flow. The course of business must not only be protected, but business processes should also be improved upon with every policy formulated.

Corporations are beginning to place greater emphasis in this area, recognizing that security policies are the backbone in substantiating a well-formed business case. The widest possible array of security equipment might still struggle to protect a system if its employees are not versed in preventive safety techniques. A policy should reflect the needs of an organization and encourage those elements that could help to grow its business. In essence, security, and its policies, should act as business enablers.

This chapter is the precursor to formal policy formulation (which is covered in detail in Chapter 10, "Essential Elements of Security Policy Development"). It explores key areas that policies should address, from equipment utilization and employee awareness programs to querying senior management on internal best practices. Most importantly, it can serve as a benchmark for ascertaining an organization's current security posture.

This chapter covers the following topics:

- Securing the organization: equipment and access
- Managing the availability and integrity of operations
- Implementing new software and privacy concerns
- Regulating interactivity through information and equipment control
- Mobilizing the human element: creating a secure culture
- Creating guidelines through the establishment of procedural requirements
- Determining rules and defining compliance
- Securing the future: business continuity planning
- Ensuring a successful security policy approach
- Surveying management

Securing the Organization: Equipment and Access

After equipment is installed and personnel are trained, spotting vulnerabilities demands the incessant task of analyzing minutiae. Whether it is log analysis, password control, physical building access, or strict rules governing departing employees, to name only a few, concentrating on details can help to ensure that security cracks are revealed and handily rectified.

The discussion in this section centers on the following topics:

- Job categories
- Departing employees
- Password sanctity
- Access

Job Categories

Many organizations use job categories to determine the scope of system access to grant individual users. A field salesperson with remote access might need to regularly check e-mail and search for marketing tools, but she should not necessarily be able to generate finance reports from the accounting department. Defining access by job category can help to preserve data integrity and ensure that unauthorized users, whether internal or external, cannot make unlawful contact with applications, operating systems, and networks.

Departing Employees

Recently departed employees can pose a risk if their access is not summarily terminated. In the flurry of activity that can surround a departure, laptops, keys, credit cards, and other physical property are collected, and the local manager might arrange to change the front door lock and forward the company credit card to the finance department. But a long-distance calling card might struggle to find its way back to the communications division. Similarly, advising the IT department to sever access privileges is not always high on a manager's alert list. Given the potential for damage that a recently departed employee could inflict, IT

notification of user de-access should be prioritized appropriately. Outlining a procedure for departing employees, even those transferring departments, ensures that unlawful, yet still authorized, access does not occur.

Password Sanctity

The process of disseminating user passwords needs to be securely controlled. Users should be instructed, if not required, to change passwords on a regular basis and to choose words or characters that are not easily identifiable. Equally important, users should extend the same respect to passwords as they do their personal bank card PINs. The sanctity of passwords is of paramount importance; mishandled, they can represent the weakest link in a once-formidable chain.

Access

Physical access continues to play a significant role in network security. Installing floor-to-ceiling barriers might be deemed appropriate to protect a server room and, depending on the organization, securing air ducts leading to the room might also need to be considered. Certain organizations might find it appropriate to institute a *clean-desk* policy, ensuring that employees remove all paper and books from their desktops before they leave work for the day. Similarly, a *closed-blind* policy can ensure that wandering eyes outside a building cannot view its interior.

Sensitive areas must be defined and access appropriately restricted, and visitors or noncompany persons must never be left to wander a building alone. A branch office of a large enterprise, the former workplace of one of the authors, was visited late on a Friday afternoon by a photocopier service technician. He approached the receptionist and informed her that he needed to perform regular maintenance on the office copier. Not wanting to disturb her any more than necessary, he asked her to point him in the direction of the copier. She gratefully complied and returned to planning her weekend, and the technician wandered down the hall to service the equipment. Moments later, the receptionist attempted to place an outgoing call, but she could not get a dial tone. She walked over to a nearby phone, but still no dial tone was available. She consulted a manager, and together they walked to the telephone equipment room. The photocopier was located in the same room, but the technician was nowhere to be seen. They immediately noticed that the rack holding the PBX telephone switching

equipment was empty. The technician had made quick work of snatching the PBX and had apparently exited through a rear door. Maintaining a strict visitor policy through the use of badges, visitor accompaniment, and employee vigilance can help to better ensure a secure environment.

Security issues can vary markedly by organization, ranging from the handling of hazardous materials to ensuring that IT equipment is protected against widespread power disruptions. Planning sessions that fully consider an organization's unique requirements can aid in forming the foundation of a well-constructed security policy.

Managing the Availability and Integrity of Operations

Maintaining availability and ensuring integrity of both physical and logical equipment are the bedrocks of operation management. Its goal is to protect the organization from interruption to its regular business activities and to minimize risk of system failure.

Safeguarding information requires that measures be in place before users begin to interact with one another or the Internet. For example, an organization could only ensure the integrity of its database if its appointed agents, typically in-house IT staff, were the sole persons responsible for loading software and performing maintenance on the system. Individual users would not be allowed to download or install software on their workstations, laptops, or local networks. IT would assume that responsibility, along with the task of deploying appropriate antivirus software throughout the network and its appliances.

IT staff would also ensure that discarded hard drives, prior to being recycled or trashed, get *sanitized*, a process that overwrites each block of a disk drive and fills it with 0s.

Safely managing the vast amount of information organizations typically generate requires that a consistent set of practices be instituted to ensure the following items:

- Systems are backed up regularly, preferably daily.
- Backed-up data is stored off-site, possibly using service providers who specialize in collecting and storing tapes and CDs. Whether in-house or third-party, storage facilities should be located in geographically secure areas.
- Thorough logs are maintained, enabling audit trails to be followed should an attack ever occur and forensic analysis required.

Managing security operations should include a systematic process of checks and balances, which can reduce the probability of unauthorized modification or misuse of equipment. Policies should ensure that no individual could perform all the following functions:

- Request a service
- Approve the required funds for the service
- Interview all vendors, contractors, or product providers
- Place the purchase order for the service or product
- Approve and make payment to the vendor
- Reorder the service

A chain of responsibility ensures that multiple individuals must give their consent before plans are put in motion. While it has the potential to become overly bureaucratic, the end justifies the means—checks and balances are the keystone of efficient operations, security or otherwise.

Implementing New Software and Privacy Concerns

This section addresses issues to be considered when implementing both custom and vendor-supplied software, and the integrity of data during transmission. The discussion centers on the following topics:

- Custom and vendor-supplied software
- Sending data: privacy and encryption considerations

Custom and Vendor-Supplied Software

The task of determining appropriate software for a company network can be challenging. Many organizations have invested untold sums assigning internal teams to test a litany of vendor offerings, only to decide that no single product could meet their unique requirements; the organizations were then relegated to writing their software. It's an expensive process that can be fraught with its own set of potential security issues.

Regardless of the route an organization might follow—in-house, custom-written software or off-the-shelf vendor-supplied software—certain fundamentals must be met. For example, extended password protection might not be of interest today, but in the future, unforeseen circumstances could force an organization to change its security posture. It is prudent to ensure that basic privacy options are included in current software and can be implemented without necessitating wholesale structural changes.

Custom programs should include the following items:

- During the development stage, creating a program that identifies potential security holes and implements an effective process to plug them
- Prior to production, running acceptance testing to root out unforeseen programming errors
- Postproduction, initiating a process that continually searches for newly created holes, and plugs them

If an organization plans to use off-the-shelf software, it is best to select a program that requires the least amount of modification. Well-known brands should have most holes plugged before the product is released to market, but by virtue of their brand-name status, these products can also attract more attention than lesser-known brands; this can result in hackers searching for holes even more diligently. In instances where issues surface after the product has a widely installed customer base, manufacturers are typically quick to issue patches to correct problems.

Postinstallation software modifications could potentially create back doors, because changes never occur in a vacuum. In typical situations, one change usually begets another, and the computing world is not immune to the domino effect of changes. The less software is modified, the fewer unexpected and unforeseen changes will result.

Change Control

A process that documents all changes, regardless of how minor a particular change might seem, can help to counter a negative impact a change might pose to a system. Commonly known as *change control*, it is a process that allows organizations to retrace their steps, from approval and security assessment of the proposed change to system backup, implementation, and monitoring of the change. Should an issue ever result from the change, determining the source of the issue should be less challenging to ascertain.

Sending Data: Privacy and Encryption Considerations

An organization might not need to encrypt every communication it sends out. Adding steps to any process naturally slows a system, and while it can seem inconsequential, encrypting and decrypting a communication still requires time and effort for both the sender and receiver.

Organizations can dictate a practice to streamline file encryption by developing a policy that states which communications are to be protected. The approach might consider the sender or the type of file being communicated. For example, a rule might state that e-mails from the CEO or files from the finance department are automatically encrypted. Conversely, an organization might consider encrypting all data it sends out, regardless of importance, to avoid inadvertently singling out its most sensitive transmissions to hackers. When a process becomes policy, less chance exists for confidential data to inadvertently be communicated in clear text.

Similar to a corporation's automatic encryption of particular users' e-mails, a program should be established that ensures the safe handling of users' public keys and certificates. The program should also include a process that revokes the keys and certificates when they are no longer required.

Regulating Interactivity Through Information and Equipment Control

Consistency is the key to effective communication of most messages. Whether it is a senior executive consistently repeating a specific objective or the simple labeling of documents to create an expectation, the need for employees to adhere to guidelines is of paramount importance.

This section considers the following topics:

- Determining levels of confidentiality
- Inventory control: logging and tagging

Determining Levels of Confidentiality

Most organizations regularly e-mail and courier envelopes and documents they deem to be sensitive in nature. Labels such as private, personal, protected,

confidential, and secret are used to ensure that documents are afforded appropriate respect. The decision to label and choose terminology is generally made by the sender.

Regulating interactivity attempts to define a process users can call upon to determine the following items:

- When a situation or file warrants labeling
- What label to use—private, confidential, secret, and other similar markers

This process sets expectations. It allows e-mail users to effectively prioritize incoming traffic. It also allows the mailroom to appropriately segregate and distribute internal mail, and reception staff to effectively handle couriers and pass confidential packages to the intended receiver or the appointed agent.

At a minimum, three security communication classifications should be used, and the security level should be noted on each segment of the communication, including the envelope, e-mail, file, and actual document. The latter is particularly important in the case of e-mailed documents, where the receiver is more likely to generate a printed copy of the confidential file. An accompanying comments section should note that sensitive documents should only be printed on a dedicated printer, when the user is available to immediately collect the documents.

Inventory Control: Logging and Tagging

It might seem odd to individuals uninvolved in the process, but maintaining up-to-date and comprehensive inventory listings of all hardware, software, and data assets can be challenging. It is particularly difficult for large enterprises with remote offices, but it is advisable to develop centralized practices or to construct a controlled decentralized process whereby every department has one IT-sanctioned individual who can perform the necessary work. The process would strive to curtail aberrant network additions and to protect the organization against unknown equipment vulnerabilities, because an IT department cannot protect equipment it does not know exists.

In an attempt to sidestep perceived bureaucracies, the following mistakes might be made:

- Departments might be tempted to purchase and install their own network equipment, unwittingly creating a possible conflict with centralized security measures.

- Departments that independently install certain equipment and software could unwittingly cause negative implications, similar to two doctors prescribing prescription drugs for a patient, although neither is aware of the other's involvement. The computing pairing would likely not result in a fatal error, but it could serve to undermine security by creating back doors.
- Users could install personal wireless hubs, enabling them to wander from their workstations but still be connected. As discussed in Chapter 2, "Crucial Need for Security: Vulnerabilities and Attacks," this could inadvertently result in a breach.

Enforcing a consistent program that logs every piece of equipment, both hardware and software, can serve to remind all employees that equipment purchases must be approved and sourced centrally. The logging and tagging of equipment can help to thwart those who attempt to undermine a company's security measures by purchasing and installing appliances and software locally. Most importantly, manufacturers issue patches for their equipment immediately upon learning of a flaw. If the IT department were not fully aware of all equipment on the company network, fundamental patches might not get applied.

Mobilizing the Human Element: Creating a Secure Culture

The development of a secure computing environment requires high-level sensing, detecting, filtering, authenticating, encrypting, and authorizing equipment to be purchased and disbursed across an organization's appliances and systems. The process of establishing an enhanced security environment reaches well beyond physical equipment in an attempt to bring together an organization's most diverse component: its people.

This section considers the following topics:

- Employee involvement
- Management involvement: steering committee

Employee Involvement

It is becoming increasingly incumbent upon organizations to foster a culture that embraces security as an employee-initiative program, rather than a set of

top-down rules imposed on users. Most employees have a genuine desire to maintain a positive working environment, and if they are informed about issues and understand what is at stake, they are more likely to become vigilant participants in the security process. Employee education can spell the difference between creating a security culture and merely installing equipment to build a security system.

Education can take many forms, but setting a tone can begin the moment an individual joins an organization. By incorporating security expectations in every job description, or statement of duties, individuals not only understand what is expected but also recognize the organization's commitment to having its employees accountable for security. The more prominence the statement is given on a job description, the greater its impact for each employee.

Orientation programs can be ideal forums to begin the process of disseminating security information, allowing new users to acknowledge the following policies of an organization:

- Internet policy
- E-mail policy
- Hardware and software policy
- Physical security policy

In recent years, organizations have become more diligent in checking business and personal character references during the hiring process. They delve deeper into resumes, substantiating employment periods, academic degrees, and other pertinent claims a prospective employee might make. Certain organizations are extending this practice to include contract, part-time, and temporary workers, ensuring that agencies that provide such people perform exhaustive identity checks before they are approved for work.

Management Involvement: Steering Committee

Organizations can have departments that are so diverse that it can be challenging to get its different factions moving in the same direction. From R&D and finance to warehousing and investor relations, finding common ground can be a challenge unto itself. While security is not the great leveler, it is an element that runs through every fabric of an operation. Every user is capable of wreaking havoc, and every individual is responsible for the sanctity of security practices.

Creating a security culture can be enhanced by the formation of an inter-departmental senior-level security steering committee. The direct involvement of leaders from distant groups can create positive ripple effects in the organization. Senior managers can do the following:

- Bring pertinent issues to the fore
- Be required to understand the needs of other departments, and the organization, in their quest to achieve a process that benefits all
- Provide a reliable litmus test to determine whether potential solutions are overly restrictive and could result in negative implications, such as users circumventing the rules
- Have a stake in the process, which makes them better equipped, and more inclined, to ensure implementation in their own departments

The steering committee concept can be a positive forum for senior managers to develop corporate policy in an area that is normally outside their sphere of influence. No single entity of an organization is an island, and bringing senior managers together under one umbrella can have a twofold effect: It can help to ensure the organization's security, and it can create an avenue for the pertinent corporate discussions that naturally ensue.

Creating Guidelines Through the Establishment of Procedural Requirements

The structure of security policies should not appreciably differ from other procedural documents an organization might construct. Policies should be formulated by a group consisting of security and company experts; the latter should comprise a cross section of senior managers who lead major departments within the organization. While Chapter 10 focuses on policy content, this abbreviated overview is concerned with fundamental structure. Specifically, every policy should attempt to answer the following questions:

- What is the policy about, and how does it get accomplished?
- Who owns the policy?

Policy Fundamentals

Every policy component should explicitly state what it is attempting to achieve. If a particular process uses technology to realize its goal, a short summary detailing the role of the equipment should be provided to enable the reader to garner its purpose. Equipment usually requires human intervention, and policies should detail all that is required of users to ensure proper use and compliance; the users need to know unequivocally what is expected of them, including the potential consequences for noncompliance.

Policies should contain defined review dates, ensuring that their core components are continually reevaluated and updated.

Determining Ownership

Every process needs an *owner*, an individual who is ultimately responsible for a function or job. Whether the process is equipment, networks, software, appliances, or databases, clearly defining roles and responsibilities can avoid the inevitability of postattack finger pointing.

The sales department, as an example, might believe that it owns the customer relationship management (CRM) software, and the engineering department might justifiably assume that it has responsibility for its highly specific plotter equipment. But the IT department likely has a different view of both situations. Should an attack be the result of improper loading or installation, which department would be at fault? Different levels of responsibility must be considered: Operators of the sales tool or engineering printer might not consider security their issue, but unless otherwise specified, owning either should entail complete accountability. To resolve this dilemma, an organization might declare two owners for specific situations: The user would be responsible for populating fields with data, and the IT department would be accountable for operability, ensuring that data is backed up every evening and that patches are applied as soon as they are published. This process would ensure that the equipment user is responsible for determining security classifications and secure handling of documents produced on the equipment, while IT is responsible for the security of the physical equipment itself.

Ownership is not about placing blame. Rather, it is concerned with assigning complete responsibility, ensuring that no individual or department can ever say, "I thought someone else was supposed to do it." Ownership defines accountability, and in so doing promotes a culture that is steeped in prevention and responsibility.

Determining Rules and Defining Compliance

Users within a corporation must abide by its rules, making it incumbent upon the organization to ensure that its policies are logical, fair, ethical, and germane to computing and security jurisprudence. Corporations must ensure that they act not only within the law but also within the spirit of the law. This section considers the following topics:

- Corporate compliance
- User compliance

Corporate Compliance

Issues have recently surfaced that bring new emphasis to the phrase "acting within the spirit of the law." Many have argued that laws governing corporate behavior shouldn't necessarily dictate strict rules of conduct, because rules can be misinterpreted, misunderstood, or simply gotten around. It is argued that because one cannot misconstrue the spirit of a law, the business community might be better served by a system that encourages adoption of that spirit.

The Internet has made various materials more accessible than ever, and certain copyrights can prove difficult to protect. While legislation is working hard to keep up with technological advancements, enforcement can be another issue. Corporations have long respected copyright laws on software, ensuring that counterfeit copies of software are forbidden on company property. But inappropriate e-mail and file deletions are still a relatively new issue, and only recently have they become synonymous with document shredding.

HR departments are using security technology to protect individuals'privacy, and corporations are making certain that all copyrights they encounter are

respected. Organizations are becoming exceedingly more diligent in all aspects of their computing environments, ensuring that compliance to laws is strictly adhered to—both to the letter and, increasingly, to the spirit.

User Compliance

User compliance, or more specifically, observance and adherence to company rules, plays a major role in security policy. The concept of "inspect what you expect" means that an organization should follow up on policy compliance and not just assume its users are following the stated rules. Whether the evaluation is log analysis or Internet tracking, the organization must check, or inspect, to ensure that rules are being followed. Note that most rules are not invasive and exist primarily for the safety of both the user and the employer.

Users are tasked with keeping company equipment safe while it is in their possession. For the typical corporate user entrusted with company property, that usually means a laptop computer. Keeping the equipment safe can run the gamut from restricting Internet browsing to appropriate sites and not loading third-party software, to ensuring that the laptop is locked when not in use. When traveling, a laptop and related equipment should be secured in a safe room. If one is not available, equipment should be placed in a locked suitcase. Thieves typically remove items from hotel rooms that are easy to conceal; suitcases are not typically stolen.

Users need to be aware of their surroundings, even when they are traveling within a city. Three employees of a large enterprise had just completed a sales call late one afternoon when they decided to have dinner before returning to their hotel. Traveling together in a nondescript sedan, their laptop computers securely hidden in the trunk, they confidently parked the car in a well-lit area and went into the restaurant for dinner. Potential criminals are everywhere, and the person watching the three clean-cut men in business suits emerge from their car at 5:30 p.m. and walk to the restaurant empty-handed, probably quickly surmised that laptop computers could be in the trunk. After dinner, the three men returned to their car to find the trunk lid damaged—and their computers gone. Security means not merely following the rules but interpreting them so they are relevant for every situation.

While organizations compile comprehensive regulations that are relevant to their mandates when determining rules for user compliance, the following guidelines are applicable to most companies:

- A clearly defined Internet policy must be acknowledged by all users.
- A system policy must be in place that clearly states unacceptable computing behavior, requiring the user to consider the spirit of a policy and not merely its black-and-white rules.
- A process must ensure that company confidential documents are never stored on a user's hard drive. Rather, any documents that are labeled private, or confidential, could only be stored on the company server, as an example.
- Wide use of monitoring tools can aid in identifying misuse. For example, intrusion detection systems (IDSs) look inside a packet to ensure that the payload is what the header claims it to be.
- The organization could provide constant reminders encouraging users to comply with safety rules, for example, pop-up screens that contain warnings, reminding users to log off when they have completed a session. Or, the organization can establish an enforced logoff after a specified period of inactivity.
- Appropriate personnel should know relevant state, local, and federal law enforcement officials.
- Appropriate personnel should be well versed in legal requirements that are germane to the specific industry to which the organization belongs, or the county in which it resides.
- If certain users are responsible for employing third-party service providers, the user responsible needs to ensure that the service provider has adequate, and auditable, security to ensure the corporation's privacy.

Lists can be endless—the challenge lies in delivering the organization's intent without the message becoming stale. By engaging in a practice that promotes continual education, users can be well versed in their employer's mandate, fully comprehending how its security posture is instrumental in helping the organization achieve its goals.

Securing the Future: Business Continuity Planning

Crises will inevitably occur. Whether they are physical, such as an earthquake or a terrorist attack, or cyber, such as a distributed denial of service (DDoS), preparedness is the key to effectively managing a crisis. The difference between falling victim to an event and working through a highly challenging time is planning.

A comprehensive continuity plan is essential in maintaining or restoring business operability. A hospital or public utility, as an example, would require a plan to maintain operations during a crisis. Conversely, a sporting goods distributor might decide to concentrate on a plan that restores its operability after a crisis has passed. The potential lost revenue might not justify the expense of a costly program that attempts to maintain operability regardless of challenges. A hospital or utility would not have a choice.

Continuity plans should consider the following items:

- Knowing the parameters of a given situation that could warrant the use of the plan
- Having a detailed inventory of standby systems, including the length of time required for each one to be fully operational
- Determining what would constitute the completion of a critical period and a return to normal operations
- Selecting an appropriate leader(s) to manage the crisis. While separate leaders could exist for technology and business requirements, one overall leader must be chosen
- Knowing the actions that need to be performed and the persons (or job functions—see next bullet) responsible for performing them
- Assigning job functions rather than specific people to specific continuity tasks so that if a person leaves a firm, the new occupant of the job function is the replacement for the continuity task
- Assigning specific reporting sites if an alarm is sounded
- Ensuring that users know the sites and are confident in their assignments, particularly if the continuity site is in another physical location
- Using the expertise of individuals, particularly the IT staff

- Formally testing the plan, rooting out all weaknesses
- Defining the amount of time needed to bring the continuity plan online
- Most importantly, keeping the continuity plan current, both in its practice and content

Continuity plans are similar to term life insurance policies: One plans for the worst but hopes never to realize the policy's payoff. A detailed and workable plan to maintain operations during trying times can allow a sense of confidence that is only achievable through comprehensive contingency planning.

Ensuring a Successful Security Policy Approach

Comprehensive security policies are tools that employees and management can use to understand how the organization is protecting itself—and what it expects from its users.

One of the main challenges in creating this type of policy is ensuring that it doesn't become overburdened with rules that could become insurmountable barriers. Note that security does remove a certain degree of flexibility. Similar to installing a home security system, the more comprehensive the system becomes, the less mobility one has in the home. A simple perimeter system that places contacts on doors and windows allows full movement within the house. But with the addition of motion detectors and laser beams, a dog's attempt to retrieve food mistakenly left on a kitchen table could conceivably trigger an alarm. The decision to install a comprehensive home system is usually preceded by a discussion centering on the real cost of vulnerability. Deciding on the makeup of the system can only begin after that discussion is concluded, because one cannot effectively mitigate risk until the person knows his level of aversion to it.

In a network environment, if users are routinely bypassing security in their rush to complete work, there could be many possible issues, including, but not limited to:

- Users are ill-informed about vulnerabilities that exist and simply bypass network security measures as a matter of course.
- The systems in place might be overkill for the type of work that needs to be accomplished.

This section attempts to pinpoint key areas where security policies have been known to be vulnerable. Keeping these points in mind when formulating policy can help to ensure its eventual effectiveness. This section examines the following topics:

- Security is a learned behavior
- Inviting the unknown
- Avoiding a fall into the safety trap
- Accounting for the unaccountable
- Workflow considerations
- Striving to make security policies more efficient

Security Is a Learned Behavior

Individuals are not born cautious. Quite the contrary; they are naturally trusting, open, and inviting. Part of the rearing process involves teaching individuals to become suspicious. Cultivating a secure environment in a computing system is not dissimilar to teaching an individual to be wary. Networks are not born cautious, as evidenced by routers that broadcast their location. Security appliances are introduced to shield vulnerable equipment, but they cannot protect users who act recklessly or sloppily; that form of preventive guarding must be learned by users.

Earlier discussions have alluded to the argument that certain organizations are better served by explaining their security posture to users. While it is challenging to fully protect a network from a user who willfully wreaks havoc, the vast majority of users who might cause harm are not doing so maliciously. They usually have no perception of the damage, or potential for damage, they have left in their wake; they simply do not know any better. An organization that openly shares its rationale for security generally finds its users less likely to skirt measures it puts in place, and a corresponding reduction in the amount of inadvertent errors it experiences should result.

Teaching appropriate security techniques takes time. Through the power of conditioning, users can learn how to properly navigate a system without putting it in jeopardy. Repetitively performing tasks and walking through the system with a knowledgeable teacher, users can become skilled at performing safe computing.

Consistent positive reinforcement, whether it is praise or ongoing education, can help to create a corporate culture that is focused on making security a learned behavior.

Inviting the Unknown

Most security systems are designed to deal with known entities, either attacks that have occurred or are feared to occur. Equipment is put in place, and an organization returns to its normal business. A comprehensive network security program dictates that minor vulnerabilities, or seemingly insignificant cracks, should be scanned for constantly, because the most harmful invasions usually come from the most unsuspected places.

Regular security scans should do the following things:

- Identify an organization's most vulnerable points, and assume that attacks could be launched against them
- Identify network areas that the IT department assumes to be highly secure, and determine their weakest links

Even the most secure environments have stress points, and identifying them is the first step in forging a more resilient network. Continually scanning for vulnerabilities in the most unsuspected places can proactively help mitigate the unknown.

Avoiding a Fall into the Safety Trap

Perfectly secure environments do not exist. Purchasing every possible type of equipment doesn't protect an organization if its users are not effectively trained. Furthermore, responsible employees cannot protect a company from a DDoS attack without the help of proper equipment. It is a combination of both that provides the most comprehensive security. Equally important is recognition that implementing security is not a one-time effort. Threats evolve and disappear, only to be replaced by new and more sophisticated ones. Policies must be able to respond quickly, efficiently, and proactively.

A security-minded organization can use a revolving wheel, as shown in Figure 5-1, to underscore its daily practices and to help it create a forward-thinking security posture.

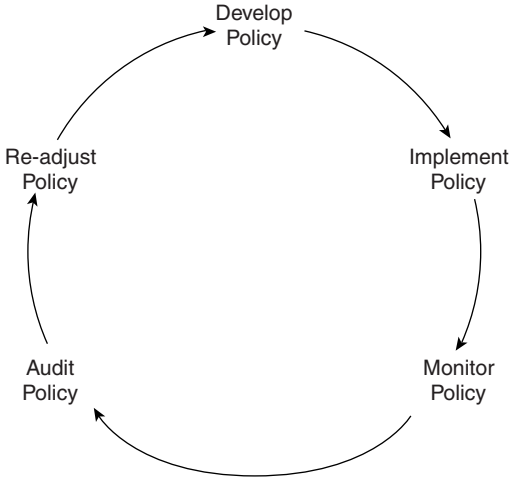

Figure 5-1 *Closing the Loop on Security: Making Policy Review a Constant*

Business environments rarely remain static, and the wheel ensures that an organization can keep pace with an ever-changing world.

Accounting for the Unaccountable

The likelihood of a hacker planning and carrying out a full-scale attack against a random network is remote. But should one occur, its effects could be devastating. Protection equipment, or the act of mitigating threats, is a type of insurance vehicle that organizations use to keep hackers at bay, as discussed in Chapter 3, "Security Technology and Related Equipment."

The most common threats organizations confront are those that come from within. Whether they are premeditated or inadvertent, the end result is usually the same. Human error can result in a nonmalicious DoS attack that, while innocent, can still bring down a network.

Some breaches might appear innocuous on the surface, but they could result in serious damage being inflicted if not immediately addressed. For example, a staffer who routinely borrows the phone line from the fax machine to dial in to his personal ISP opens an unprotected path to the Internet that a hacker could

recognize. The staffer might know he is not allowed to do this, but his need to connect to his personal account through the ISP could outweigh his misgivings, particularly if he isn't reprimanded after the first few times. The more he accesses his ISP and gets away with it, the more bravado he will have to continue.

Aberrant activity must be addressed in security policies so that users can understand the spirit of what is expected of them.

Workflow Considerations

Ideally, policy formulation teams should include users who are familiar with an organization's workflow to ensure that a policy reflects the workflow.

Policies that reflect workflow have the added benefit of addressing rules that are too cumbersome for users by avoiding the pitfall that is all too common with restrictive regulations: Users go around them and typically create back doors in the process.

Security policies that take practical considerations into account have a greater potential to effect positive results.

Striving to Make Security Policies More Efficient

Identifying and planning for the natural weaknesses in security policies can be an effective tool to use when creating a comprehensive plan.

Breaches can be avoided when planners model a process before committing it to implementation. For example, a procedure might reasonably dictate that a particular room remain locked during business hours and assign responsibility for the key to one person. But if multiple users require access to the room to carry out their normal course of duties, frustration could ensue if the individual in charge of the key is not always readily available. Users might find a way to circumvent the rule by surreptitiously copying the key. It is understandable that the organization might need to control access to the room, but rather than creating an environment that inadvertently encourages underhanded activity, it could research more reasonable access measures, such as the authentication and authorization tools described in Chapter 3.

Ensure that a process exists to routinely review policies. Even the best-laid plans can require tweaking, and security policies should not be immune from postimplementation analyses. Organizations can also change in size, structure, and equipment that they use; policies should be flexible enough to appropriately reflect any relevant changes to the corporation.

Continue to educate users on the importance of security and on what they can do to help. Most employees have strong positive feelings about their employer and, if possible, they genuinely want to make a difference in their workplace. An environment that encourages its employees to become active participants in the security process will be well structured to deal with threats in the future.

Surveying IT Management

Making the business case for network security requires that a multitude of soft factors be garnered from both the technical and human elements within an organization. While technical elements are relatively straightforward to ascertain, determining human elements can be more challenging, because personal opinion can vary markedly across an organization's senior management team.

To begin the process of determining an organization's tolerance for risk, a series of questions were developed for this book. The questions, presented in the Infosec Management (IM) survey, were created to address a fundamental requirement of most organizations—a company must first acknowledge its aversion to risk before it can begin the process of effectively securing itself. This section discusses the need for determining a consensus on risk and then presents the IM survey.

The discussion centers on the following topics:

- The need for determining a consensus on risk
- Infosec Management survey
- Infosec Management quotient

The Need for Determining a Consensus on Risk

Successful companies typically follow similar paths: A senior-level consensus on goals is established, and then managers work diligently to achieve

the stated goals. While individual drive and entrepreneurial spirit are essential factors in every company's success, a firm's senior management team must first reach consensus on the organization's goals and strategies; consensus is simply the surest way to underwrite success. Developing an effective security plan is no different; it requires an organization's senior management team to first reach consensus on its aversion to risk.

It is important to acknowledge that achieving consensus on risk is not a straightforward task. Risk is relative. Every senior manager, unwittingly or not, brings to bear on the organization his or her own personal tolerance level for risk. To achieve effective risk management, every significant senior manager needs his or her opinion to be considered. The IM survey, which is discussed in the next section, was developed to ensure that organizations can achieve consensus for the establishment of their security postures.

Infosec Management Survey

The Infosec Management (IM) survey in this chapter and its sister Infosec Operational (IO) survey, which is presented in Chapter 7, "Engaging the Corporation: Management and Employees," were created for this book to help organizations determine their overall aversion to risk. The IM survey is designed to be completed by IT managers, CIOs, CSOs, and CISOs. The IO survey is designed to be completed by senior managers from every significant department. Material for the surveys reflects issues that are discussed in this book, ranging from policies, processes, and business requirements to equipment and personnel issues. While the survey questions are designed to be applicable to most organizational situations, the manager responsible for disseminating the survey should feel free to change the questions to best reflect his organization's requirements.

The IM survey focuses on policy and the human aspect of risk management; the results can help calculate an IM quotient. The IM quotient is the mean score of all those who participate in the survey. The IO survey in Chapter 7 focuses on technology, equipment loss, and communication; the results can help calculate an IO quotient—the mean score of all those who participate in the survey in Chapter 7. The IM quotient and IO quotient are part of the risk-aversion discussions in Chapter 8, "Risk Aversion and Security Topologies."

Through careful consideration of the results to answers in both surveys, managers can determine whether their current policy does the following things:

- Reflects their immediate needs
- Is flexible enough to adapt to a fluid business environment and a changing security posture
- Reflects the workflow but doesn't attempt to control it
- Has input from every corner of the organization
- Has support of corporate management
- Has an automatic review and readjustment process
- Acts as a business enabler

In addition to establishing an IM quotient and an IO quotient, the surveys aid organizations in highlighting stress points, revealing vulnerabilities that should be addressed in both policy and actions.

Organizations are encouraged to benchmark their results against industry standards, in particular ISO 17799, "Code of Practice for Information Security Management," an auditable standard first published in 2000 by the International Standards Organization (ISO). The ISO (http://www.iso.org/iso/en/ISOOnline.frontpage) is synonymous with quality benchmarking, and its work in the security field addresses similar concerns. It provides a process that deploys security standards that organizations can follow and, ultimately, audit.

The rating scale in Table 5-1 should be used to respond to the Infosec Management (IM) survey questions.

Table 5-1 *IM Survey Rating Scale*

Rating Scale	Rating Explanation
0	Not applicable, firm does not engage in process
1	Meets some requirements
2	Meets most requirements
3	Meets all requirements
4	Overachieves requirements
5	Exceptionally forward-thinking, exceeds all requirements

The survey, shown in Table 5-2, should be distributed to all appropriate IT managers: CIO, CSO, CISO, and so on. It is best to include as many senior IT managers as possible to ensure that consensus can be effectively achieved.

Table 5-2 *IM Survey*

Question or Situation to Be Considered	**Rating Schedule**
Does the organization have a comprehensive security policy that encompasses all departments, remote offices, and personnel?	5 4 3 2 1 0
Aside from denying access to finance and HR, does individual network access differ markedly by job category?	5 4 3 2 1 0
For recently departed employees, is IT notified, as dictated by policy, either before or within minutes of departure?	5 4 3 2 1 0
For intracompany employee transfers, is IT notified, as dictated by policy, either before or within minutes of transfer?	5 4 3 2 1 0
Are users prevented from reusing passwords?	5 4 3 2 1 0
Are users denied the ability to use either their first or last name as a password?	5 4 3 2 1 0
Are passwords changed, at a minimum, every 30 days?	5 4 3 2 1 0
Are visitors and noncompany personnel accompanied at all times?	5 4 3 2 1 0
Are branch or remote office employees denied the ability to install software on their computers and equipment?	5 4 3 2 1 0
If users are not allowed to load any type of software, is this mandate enforced by policy and practice?	5 4 3 2 1 0
Does IT have the sole responsibility for all software installations on all equipment, regardless of how innocuous the loading might appear?	5 4 3 2 1 0
Are discarded hard drives *sanitized,* a process that overwrites each block of a disk drive and fills it with 0s?	5 4 3 2 1 0
Are comprehensive system logs recorded?	5 4 3 2 1 0

Table 5-2 *IM Survey (Continued)*

Question or Situation to Be Considered	Rating Schedule
Are comprehensive system logs regularly monitored for abnormal behavior?	5 4 3 2 1 0
Does the organization use encryption when forwarding all confidential files and documents?	5 4 3 2 1 0
Does the organization use digital signatures?	5 4 3 2 1 0
Does IT prioritize the patching of pertinent equipment when notified by a patch information service or the vendor?	5 4 3 2 1 0
Does IT apply patches within hours of the patch being released?	5 4 3 2 1 0
Does a backup person exist to monitor and immediately install patches if the appointed person is unexpectedly absent?	5 4 3 2 1 0
Does the organization regularly (at least once per year) survey all departments and remote offices for mandatory equipment logging and tagging?	5 4 3 2 1 0
Do all users unequivocally understand the company's Internet and e-mail policies?	5 4 3 2 1 0
Are the company's e-mail and Internet policies enforced?	5 4 3 2 1 0
Does the organization have a body, or group, that is independent of IT to oversee system security?	5 4 3 2 1 0
Does every process, equipment, and policy have an unequivocal owner?	5 4 3 2 1 0
Does the organization have a policy requiring remote users and travelers to effectively secure their equipment when out of the office?	5 4 3 2 1 0
Does the organization have a formal and continuous security education program that highlights user responsibility?	5 4 3 2 1 0
Does the organization have consistent communication with employees about known security incidents/ breaches—particularly how to prevent recurrences?	5 4 3 2 1 0

continues

Table 5-2 *IM Survey (Continued)*

Question or Situation to Be Considered	Rating Schedule
Does the organization have a formal process that comprehensively vets (confirms work history, education, and so on) all employees, including contract workers and temporary staff?	5 4 3 2 1 0
Does the company have a business continuity plan in the event of a crisis?	5 4 3 2 1 0
Is the business continuity plan tested and deployed in a mock trial at least annually?	5 4 3 2 1 0
Does the organization have a process to regularly review security policies and adjust them to reflect any change in equipment, processes, or business requirements?	5 4 3 2 1 0
Is the formal security review process performed by a company-wide group that consists of business and IT managers?	5 4 3 2 1 0
Does the company fully explain its security rationale to employees so that individuals can become active proponents?	5 4 3 2 1 0

Infosec Management Quotient

The Infosec Management (IM) quotient is derived by averaging the scores of those managers who participated in the survey. Extensive IT management participation can help ensure an IM quotient that is truly reflective of the organization's aversion to risk.

The IM quotient (and IO quotient, which is determined in Chapter 7) can be married to a hard-number formulation process that helps quantify security decisions. These formulations are explored in Chapter 8 and form the foundation of the return on prevention (ROP) model.

To establish the IM quotient, determine the average score and convert it to a percentage, as follows:

IM quotient = Average of survey results * (100 / Total possible points)

where Total possible points = 5 * Number of questions

If you use all 33 questions from the survey in this chapter, the formula would be as follows:

IM quotient = Average of survey results * (100/165)

Reserve the result for use in Chapter 8 to aid in determining the organization's risk and risk aversion and to determine the appropriate topologies to avert that risk.

Summary

Policy plays an integral role in security effectiveness. Educating users on their responsibility to enhance security can have a twofold effect: It ensures that deployed equipment can perform tasks with greater effectiveness, and it creates an environment that encourages and supports individual responsibility.

The business case for network security requires that soft elements be acknowledged, considered, and ultimately weighted through adoption of an analytical process. Risk, and aversion to it, must be quantified before effective programs can be developed and put in motion. It is a fundamental step in the process of formulating concrete ROP results.

This chapter focused its discussion of policy on the following topics:

- Outlining steps to secure the physical organization, both equipment and access
- Understanding the importance of operations management of physical and logical equipment
- Safely deploying new software and understanding privacy concerns
- Promoting the need for consistent confidentiality labeling and equipment tagging
- Understanding the need to mobilize the human element within an organization to create a security culture
- Defining policies, detailing pertinent processes, and assigning ownership
- Exploring corporate and user compliance
- Developing a process to work through crises, using business continuity planning

- Acknowledging common vulnerabilities in security policies
- Introducing a fundamental step to quantify soft issues: surveying senior management

The next chapter advances the discussion by focusing on the board and presenting the issues inherent in security governance. Chapter 7 focuses on the IT manager, providing him with an overview of the business side of the organization and equipping him with the necessary tools to effectively lobby his senior-management colleagues on the merits of investing in security. Chapter 7 also introduces the next survey, the Infosec Operational (IO) survey, the results of which are explored in Chapter 8.