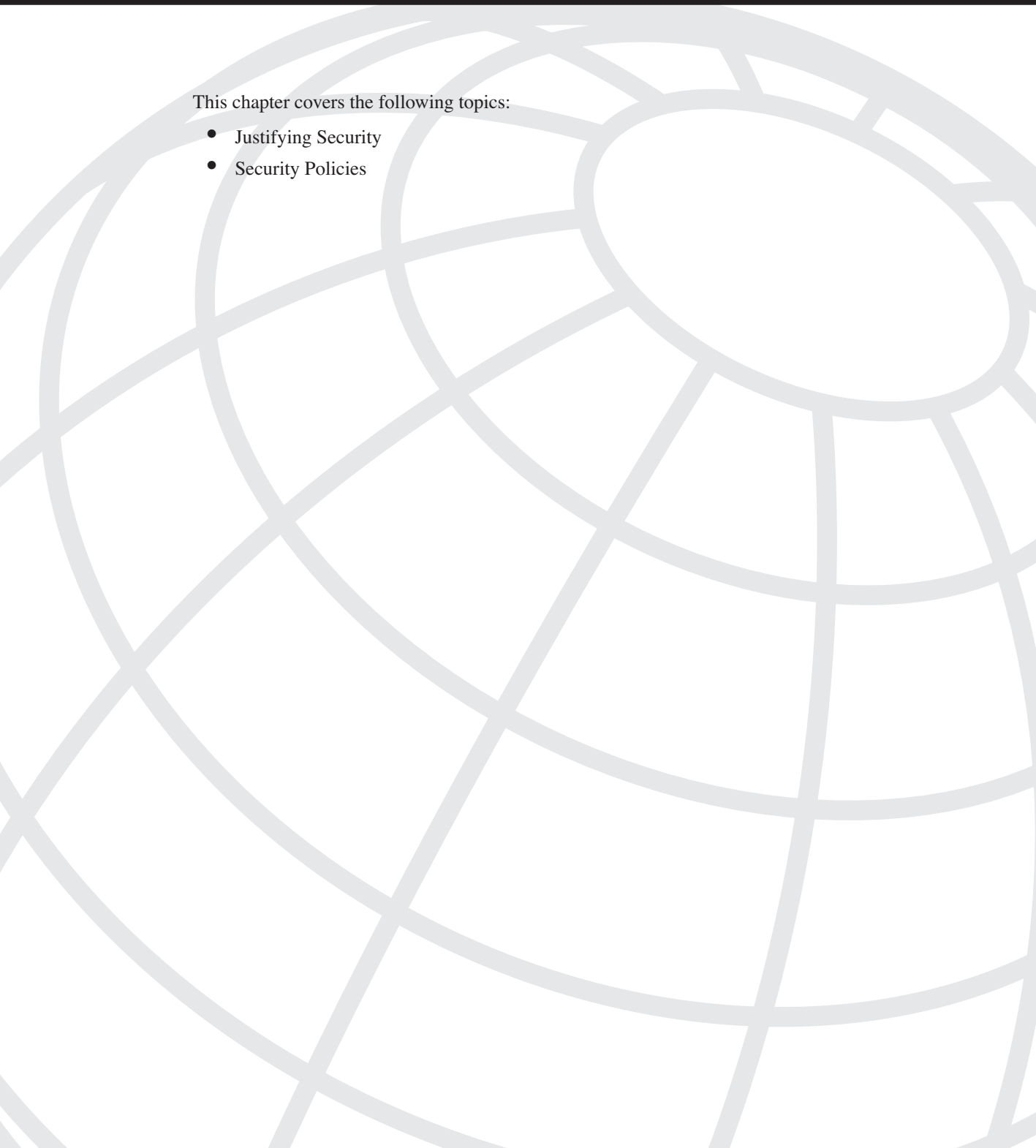
This chapter covers the following topics:

- Justifying Security
- Security Policies



CHAPTER 2

Security Policies

If you don't know where you're going, there is no way to calculate the best route to follow.

This chapter presents a way for you to decide what your security goals are and establish, implement, and enforce the security rules that will help you achieve them.

Justifying Security

Security is expensive. Before allocating funds, senior management will want to know what they are buying, what it will protect, and what alternatives they have. This section presents the tools you need to answer those questions.

Security Defined

The following is a good definition of security:

> "Tools and techniques that prevent unauthorized people or processes from doing anything with or to your data, computers, or peripherals."

Security is not a firewall or cryptography or a virus scanner; although, they are all components of a security solution. It is a process that examines and then mitigates the risks that arise from your company's day-to-day activities.

Kinds of Security Risks

Risks come in a wide variety of forms. Here are some examples:

- Loss of assets (theft)
- Service disruption (business interruption)
- Loss of reputation (disparagement)
- Expenses of recovery (profitability impact)

Shareholders expect managers to protect or enhance the value of the company. Security breaches that affect any of these items violate shareholders' expectations.

NOTE Another kind of risk is just now emerging: the risk of running afoul of the law.

Many new laws include punitive measures (usually fines). Three examples from the United States are Graham-Leach-Billey, which affects U.S. financial institutions and requires disclosure of privacy policies to customers; the Health Insurance Privacy and Portability Act (HIPPA), which restricts disclosure of health-related data along with personally identifying information; and the Electronic Communications Privacy Act (ECPA), which specifies who can read whose e-mails under what conditions.

Knowing the Enemy

A common security mistake is to assume that attacks always come from outside your organization. Many companies do the technological equivalent of digging a deep moat around the organization and filling it with hungry alligators, then leaving the interior doors unlocked.

You might like to assume that hackers are nearly all pimply-faced, teenagers. This just isn't so. A few artists can find security flaws in systems and exploit them. Some of those talented-but-misguided individuals codify their exploits into scripts and release them on the Internet where a subclass of hackers, known as *Script Kiddiez,* try to use those scripted exploits. The bad news is that there are a lot of those "Kiddiez." However, the very fact that they are scripted attacks makes them easy to detect and often fairly simple to defend against. (See Chapter 11, "Maintaining Ongoing Security," for details.)

Your ID Badge gets you in through the front door and into your work area. It also prevents you from going where you are not allowed. As a society, we've had hundreds of years of experience designing physical security systems (which still get breached, by the way). Computers have been with us for only a few decades; computer networks even less time.

A CSI/FBI study (conducted annually, available at www.gocsi.com) states that more than half of all intrusions are by insiders. Security professionals have to work a lot harder to protect their organizations against this class of intruders. By and large, they are more sophisticated computer users. Even worse, they already have valid credentials that allow them access to the network. You have to apply the restricted-area-badge concept to your internal networks, as well. Many of the chapters in this book are specifically aimed at protecting against this internal user threat. Chapter 6, "Enhancing the FTP Server," is a prime example. In it, you learn (among other things) how to encrypt FTP logins so that insiders cannot listen in and steal other users' credentials.

The C-I-A Triad

A computer security professional's job can be described as *protecting CIA* or *maintaining CIA*. The letters and their definitions are as follows:

- **Confidentiality**—Making sure that data is not disclosed in an unauthorized manner, either intentionally or unintentionally.

- **Integrity**—Giving the following assurances:
  - Modifications are not made by unauthorized people.
  - Unauthorized modifications are not made by authorized people.
  - The data is internally and externally consistent. (That is, the data matches up with other data and with real-world experience.)
- **Availability**—Providing the reliable and timely access to data or computing resources by appropriate authorized personnel.

NOTE The opposite of CIA is D-A-D, which stands for Disclosure, Alteration, and Denial.

Approaches to Risk Analysis

You (or your management) can take five approaches with regard to any risk:

- **Accept the risk**—You must accept the risks in the following two cases:
  - You cannot do anything about the risk (for example, a vendor goes out of business or a product is dropped).
  - The cost of mitigation is not economical.
- **Defend against the risk**—You can deploy firewalls, antivirus products, encryption technologies, and so on. You can also establish procedures and policies, as discussed later in this chapter.
- **Mitigate the risk**—Even if you assume that there is no such thing as a web server that cannot be broken into, you still don't have to just accept the risk. Some of the things you can do include the following:
  - You can reduce the harsh effects of a successful break-in by being ready to reinstall the web server at a moment's notice.
  - You can take steps to maintain the web server's security. (This is the subject of Chapter 11.)
  - You can regularly audit its contents.
  - You can examine its logs.
- **Pass on the risk**—You can ensure against the risk (sometimes).
- **Ignore the risk**—This is the only foolish choice. Ignoring the risk is not the same as accepting it. Ignoring it is merely hoping that someone else will be attacked.

Three of these (accepting, mitigating, and passing on the risks) are examples of threat reduction techniques. Reducing the threat is made easier if the proper security stance is selected. With every defense, you will use one of the following approaches:

- Permit nothing (the paranoid approach).

- Prohibit everything not specifically permitted (the prudent approach).
- Permit everything not specifically prohibited (the permissive approach).
- Permit everything (the promiscuous approach).

Of these, the prudent choice makes the most practical sense and is the assumed approach of this book. It is the one that most vendors choose. For example, Cisco access lists automatically deny everything not specifically permitted.

NOTE The following story is well known among security practitioners.

Student–to–instructor: How do you configure a firewall?

Instructor–to–Student: Deny everything and wait for the phone to ring.

Solving Security with Technology

Bruce Schneier, in *Secrets and Lies, Digital Security in a Networked World,* states,

> "If you think that technology will solve your security problems, then you don't understand security and you don't understand your problems."

Security includes a necessary mindset for every employee and specified procedures to follow, in addition to technology, to minimize the risk.

Security Policies

Security policies help you define the level of security that is acceptable in your organization; they set a standard of care for every employee (and contractor).

Security policies help you plan. Without them, there would be no way to tell which security decisions help increase your security and which are wastes of time and money. Even worse, there would be no way to identify areas that were overlooked.

In this section, you learn what goes into a security policy, how to create one, and how to make sure that it is kept up to date and used effectively.

Contents of a Security Policy

A security policy is a document. Although typically approved at the highest levels, it is not a high-level document (like a Mission Statement). Your security policy defines the resources that your organization needs to protect and the measures that you can take to protect them. In other words, it is, collectively, the codification of the decisions that went

into your security stance. Policies should be published and distributed to all employees and other users of your system. Management should ensure that everyone reads, understands, and acknowledges their role in following the policies and in the penalties that violations will bring.

NOTE When separate policies deal with secure networks, publication of those policies should be restricted to individuals who have authorized access to those networks.

Security policies should emphasize what is allowed, not what is prohibited. Where appropriate, examples of permitted and prohibited behavior should be supplied. That way, there is no doubt; if not specifically permitted by the security policy, it is prohibited. The policy should also describe ways to achieve its goals.

Example 2-1 is an example of a security policy for passwords. This example is divided into several sections, for which Table 2-1 lists the sections and describes their content.

Table 2-1 *Generic Description of a Security Policy's Contents*

Section Name	Content Guide
1.0 Overview	Justifies the reason for the policy and identifies the risks the policy addresses.
2.0 Purpose	Explains why the policy exists and the goal that it is written to accomplish.
3.0 Scope	Defines the personnel covered by the policy. This might range from a single group in a department to the entire company.
4.0 Policy	This is the policy itself. It is often divided into several subsections. Examples are commonly used to illustrate points.
5.0 Enforcement	Defines the penalty for failure to follow the policy. It is usually written as "everything up to and including…" so that a series of sanctions can be applied. Dismissal is typically the most severe penalty but, in a few cases, criminal prosecution should be listed as an option.
6.0 Definitions	Any terms that might be unclear or ambiguous should be listed and defined here.
7.0 Revision History	Dates, changes, and reasons go here. This ties into enforcement in that the infraction should be measured against the rules in place at the time it occurred, not necessarily when it was discovered.

Example 2-1 *A Sample Security Policy (Covering Passwords)*

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Example Corporation's entire corporate network. As such, all Example Corporation employees (including contractors and vendors with access to Example Corporation systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Example Corporation facility, has access to the Example Corporation network, or stores any non-public Example Corporation information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the Information Security Department administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv3).
- All user-level and system-level passwords must conform to the guidelines described below.

Example 2-1 *A Sample Security Policy (Covering Passwords)*

4.2 Guidelines

A. General Password Construction Guidelines Passwords are used for various purposes at Example Corporation. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, sports teams, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Example Corporation", "EXMC", "BigApple" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

NOTE Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

continues

Example 2-1 *A Sample Security Policy (Covering Passwords)*

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards Do not use the same password for Example Corporation accounts as for other non-Example Corporation access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Example Corporation access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Example Corporation passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Example Corporation information.

Here is a list of *don'ts*:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to the Information Security Department and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the Information Security Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards Application developers must ensure their programs contain the following security precautions. Applications:

Example 2-1 *A Sample Security Policy (Covering Passwords)*

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users Access to the Example Corporation Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnTheBridgeWas*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, Notes administrator).

7.0 Revision History

NOTE In part 4.2-A in Example 2-1, there is a line suggesting that the name of the company, the nickname of a nearby town, or a stock symbol (which was unassigned at the time of this writing) are poor passwords, and they are. Other poor password examples will come from your own environment. For example, the word *bulldog* is far less secure at Mack Truck (where it is the company's mascot) than at any other company. You should expand that section with locally bad choices. If your company is national or international, you need to make it clear that there are classes of bad choices.

In large organizations, security policies are multipart documents, each referring to one or more of the others. For example, in a policy on router security, the section on choosing router access passwords will refer to the password policy.

Policies commonly apply to less than all sections of the organization. Policies on acquiring commercial software or running a test lab or training department apply only to segments of the company, whereas policies such as an Information Sensitivity Policy (deals with keeping confidential company information private) or Password Policies apply across the enterprise.

Example Security Policies

Several model security policies are available on the web. A good starting place is RFC 2196, "Site Security Handbook," which discusses all aspects of security policies, from content development to implementation. Another source of sample policies comes from SANS. The direct link is www.sans.org/newlook/resources/policies/policies.htm. If the link breaks, key the title of the page, **The SANS Security Policy Project**, into the search-this-site box on the SANS home page. Table 2-2 lists many of the policies you'll find there, along with a description of what they're for.

Table 2-2 *Common Security Policies*

Policy Name	Description
Acceptable Encryption	Provides guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, provides direction to ensure that applicable laws and regulations are followed.
Acceptable Use	Outlines who can use company-owned computer equipment and networks. It covers company computers located on company premises as well as computers located in employee's homes.

Table 2-2 *Common Security Policies (Continued)*

Policy Name	Description
Analog Line	Explains the analog and ISDN line acceptable use and approval policies and procedures. Separate rules apply to lines that are connected for the sole purpose of sending and receiving faxes and lines that are connected to computers.
Application Service Providers	Describes the company's Application Service Providers (ASPs) requirements. (ASPs combine hosted software, hardware, and networking technologies to offer a service-based application.) It refers to and incorporates the separate ASP Standards Policy.
ASP standards	Defines the minimum-security criteria that an ASP must meet to be considered for use.
Audit	Provides the authority for members of the Information Security Department team to conduct a security audit on any system owned by the company or installed on the company's premises.
Automatically Forwarded Email	Prevents the unauthorized or inadvertent disclosure of sensitive company information.
DB Credentials	States the requirements for securely storing and retrieving database usernames and passwords (that is, database credentials) for use by a program that will access a database running on one of the company's networks.
Dial-in Access	Establishes rules that protect electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.
Extranet	This document describes the policy under which third-party organizations connect to the company's networks for the purpose of transacting business.
Information Sensitivity	Helps employees determine what information can be disclosed to nonemployees, as well as the relative sensitivity of information that should not be disclosed without proper authorization.
Internal Lab Security	Establishes information security requirements for labs to ensure that confidential information and technologies are not compromised, and that production services and other interests are protected from lab activities.
Anti-Virus	Establishes requirements that must be met by all computers connected to the company's networks to ensure effective virus detection and prevention.

Table 2-2 *Common Security Policies (Continued)*

Policy Name	Description
Password Protection	Establishes a standard for creating strong passwords, the protection of those passwords, and the frequency of change.
Remote Access	Defines standards for connecting to the company's network from any host. These standards are designed to minimize the potential exposure to damages (such as the loss of sensitive or confidential company data, intellectual property, damage to public image, damage to critical internal systems, and so on).
Risk Assessment	Empowers the Information Security Department to perform periodic information security risk assessments to determine areas of vulnerability and to initiate appropriate remediation.
Router and Switch Security	Describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity.
Server Security	Establishes standards for the base configuration of internal server equipment that is owned and operated on company premises or at web-hosting locations.
Virtual Private Network	Provides guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the company's corporate network.
Wireless Communication	Establishes standards for access of the company's network via secured wireless communication mechanisms.

Creating Your Own Security Policy

Creating security policies is a four-step process:

Step 1 Decide on your level of trust.

Step 2 Define appropriate behavior.

Step 3 Create a policy review team.

Step 4 Use the work of others.

The sections that follow examine each of these steps in greater detail.

Step 1: Decide on Your Level of Trust

Assuming that people will do the right thing is easy and tempting. Don't let yourself take this shortcut. Spell out what is expected and what is prohibited. Decide on the controls you will use to measure adherence to the good practices that you are about to define. (This

applies to programs as well as people.) Specify repercussions that will follow if employees do not adhere to practices. Trust different employees in different ways. Those with unprivileged access are in a different category than those with high levels of access privilege.

Step 2: Define Appropriate Behavior

Whether the topic is email usage, password policies, or keeping company secrets, your system's users and the people who evaluate them must know what is expected. Your policies are necessary to support an HR action in the face of inappropriate behavior, or even to prosecute a criminal case in extreme examples.

Step 3: Create a Policy Review Team

The members of this team are responsible for drafting new policies and revising existing ones. Table 2-3 describes the representatives and their roles.

Table 2-3 *Members of the Policy Review Team*

Representative From	Duties
Management	Someone who can enforce the policy. This is often a senior member of the HR staff.
Information Security Department	Someone who can provide technical insight and research.
User Areas	Someone who can view the policies the way a user might view them.
Legal Department	Possibly part time, but someone who can review policies with respect to applicable laws. For multinational firms, this review is exponentially more complicated.
Publications	Someone who can make suggestions on communicating the policies to the organization's members and getting their buy in. Also, a good writer is always helpful.

Step 4: Use the Work of Others

The previous section gave a pointer to a set of policies suitable for a large company. A Google.com search turns up literally dozens of sample policies for sale. Amazon has several books. You should investigate these resources and find one that matches your organization's profile. This will save you significant amounts of work. Even more important, it will keep you from accidentally omitting vital areas from consideration.

TIP *Information Security Policies Made Easy* (Version #8), an excellent book on security policies by Charles C. Wood, comes with a CD containing policies you can edit and use. The only drawback is its relatively high cost (currently $595 U.S.).

Key Topics for Security Policies

Many of the security policies listed in Table 2-2 have key clauses that should be included, as further described in Table 2-4.

Table 2-4 *Key Policy Provisions*

Policy Name	Key Provisions
Acceptable Encryption	Tells employees how to use encryption to protect information in transit (both over the network and via laptop). Names encryption products, algorithms, and strengths.
Acceptable Use	Lists appropriate use of computing resources. Users should be made to read and sign. Contains rules for e-mail, newsgroups, web surfing, and nonbusiness use. Also states users' responsibilities regarding data in their private spaces.
Analog Line	Discusses who can have analog lines installed, for what purpose, and the things that they must do to protect the network while the line is in use.
Application Service Providers	Defines minimum-security standards to which ASPs must adhere to be eligible to contract with the company.
Automatically Forwarded Email	Discusses whether accessing, maintaining, and forwarding company e-mail to private accounts is allowed.
Information Sensitivity	Tells users how to treat company confidential, company officer eyes-only, company trade secret, third-party private and other classifications of private information.
Internal Lab Security	Sets rules that protect the main network from work done in the lab.
Anti-Virus	Lists baseline rules for using antivirus products (AVPs) and frequency of updates. Explains procedure to follow after becoming infected. Includes rules for downloading software and for allowing attachments.
Password	Covers minimum length, change periods, techniques for creating good passwords, and mistakes to avoid.
Remote Access	Acceptable use might differ for users working from home. Using company facilities to reach out to the Internet might or might not be okay. Allowing family members to use the computer and access lines is another decision you need to make and convey.
Router Security	Deals with storage of router passwords and with minimum access control list requirements.
Wireless Communication	Deals with maintaining security when sending data across wireless LANs and the rules for when this might or might not be done (and, if done, how to implement it).

Effectively Implementing Your Security Policy

When you develop policies, you need to balance productivity and security. The goal of all good employees is to get their work done. If you create a rule that the employee thinks is just in the way, that employee will either ignore it or bypass it. Sometimes, you can implement technical controls to make sure that policies are followed (password change periods, for example), but other times you cannot. (A rule about never giving your password to someone else cannot be enforced by software.) You must make security a part of the corporate culture.

This does not have to be done in a punitive way. Here are two examples.

A company whose policy called for password-protected screen savers or locked workstations whenever an employee was not using the PC was enforced by having security staff (uniformed guards on patrol) write "*tickets*"—they looked like parking tickets—and taping them to the monitor. The tickets reminded the users of the rules. The guards were taught how to Ctl-Alt-Del and pick **Lock Workstation**, and were instructed to do so whenever issuing a ticket.

Another company had guards walk around after the close of business looking for laptops left unattended. They took laptops they found and left a "*luggage receipt*" on the desk saying that the lost luggage could be claimed at the security station.

Avoiding Failure

One sure way to make a policy fail is to apply it unevenly. If certain people, because of their position or influence, can bypass policies with impunity, the policies will all become unenforceable. You must get management buy-in, even if doing so is painful.

Practice What You Preach

As a consultant, the worst project I took on was a virus extermination task. This was in the early days of networking, small hard drives, and extensive use of floppies. I went in and disinfected the server, the workstations, and every floppy in plain sight. I was not allowed to open desk drawers. I also installed an antivirus product (AVP) on every PC. (It installed in the *autoexec.bat* file.)

A week later, I was called back because the virus had resurfaced. I found two problems. One was that a floppy in a desk drawer was infected, and the other was that the user disabled the AVP because it made the PC take too long to boot up. I redisinfected, this time with permission to open desk drawers and was accompanied by a security guard. I also recommended that management implement a policy stating that disabling the AVP would result in termination. They agreed.

Two weeks after that, I was called back. This time, I traced the problem to the office of a vice president of the company who brought an infected floppy from home and disabled the

AVP. I asked the CIO if the VP was going to be dismissed. He laughed and said that the VP was too valuable to let go and that I should just clean it up and forget about it.

By the way, there was another solution that they could have employed. During World War II, General George S. Patton was made to apologize publicly to his troops—the alternative being court martial and disgrace. He apologized. (That might have been harder on him than the court martial.) By doing that, General Eisenhower kept a commander who really was too valuable to lose, but he also made it clear that no one was above the rules. I suggested that the company follow this model by making the VP send a *mea culpa* note to everyone as an alternative to dismissal. They declined.

I told them not to call me again.

Summary

This first part of the book set the stage with a chapter on essential information and a chapter on security policies. Part II deals with things you should do to harden the server software before installing a web server.