1 What Information Security Policies Are

A CLIENT CALLED ME UP ONE DAY AND asked me to come to his office. Once I arrived, he asked me to install a firewall so that his network would be secure. I asked him for his company's security policy so I could configure the firewall. He gave me a curious look and asked, "What do I need that for?"

In the years since the explosion of the Internet, this response is still the rule rather than the exception. Companies have comprehensive employee policies, sometimes filling two-inch binders, but do not have information security policies. If they do, they will hand you 5 sheets of paper that cover the assets of a multimillion-dollar corporation.

Just as employment policies describe the practices that employees and managers must take, security policies describe how the company wants to protect its information assets. That is an important concept to remember: Information is an asset. You might not be able to assign it a value, but your competitors might pay thousands or even millions of dollars to understand or even steal those assets.

About Information Security Policies

Information security policies are high-level plans that describe the goals of the procedures. Policies are not guidelines or standards, nor are they procedures or controls. Policies describe security in general terms, not specifics. They provide the blueprints for an overall security program just as a specification defines your next product.

Questions always arise when people are told that procedures are not part of policies. Procedures are implementation details. A policy is a statement of the goals to be achieved by procedures. General terms are used to describe security policies so that the policy does not get in the way of the implementation. For example, if the policy specifies a single vendor's solution for a single sign on, it will limit the company's ability to use an upgrade or new product. Although your policy documents might require the documentation of your implementation, these implementation notes should not be part of your policy.

Why Policies Are Important

Although policies do not discuss how, properly defining what is being protected assures that proper control is implemented. Policies tell you what is being protected and what restrictions should be put on those controls. Although product selection and development cycles are not discussed, policies will help guide in product selection and best practices during development. Implementing these guidelines should lead to a more secure system.

When management participates in the creation of information security policies, it demonstrates that management supports the effort, lending credibility to the entire security program. Having management support is always important. Without leadership, employees will not take policies seriously. Therefore, if you do not have the support of your upper management, your program is doomed to fail before you finish writing the policy.

> **How You Gain Management Support**
>
> First you can try to reason with them. You can point out that the systems and data have real costs. You can demonstrate how an outsider or a disgruntled insider can easily access sensitive information that could damage the company's business functions. You can show them studies, articles, even this book. But if this doesn't convince them, you might have to wait until your first disaster.

Management might say that everybody is responsible for his or her own security. That might work in the short term, but it prevents the company from working with itself. If one department uses one standard and another department uses another standard, interoperability could be a problem. Policies ensure that the company uses the same standards in every security instance. This consistency makes it easier for the company to integrate, interact with customers, and maintain a sense of security throughout the system.

Finally, an information security policy will help avoid liability. We live in a litigious society. If you try to enforce rules that are not expressly written, you will be sued. If you fire an employee for security violations that have never been written, presented to the employee, or previously enforced, that employee also can sue your company. I know it sounds harsh, but the reality can be devastating when the subpoena arrives.

When Policies Should Be Developed

Ideally, the best time to define your policies should be before your first security problem. By doing this early, your security administrators will understand what to protect and what enforcement measures can be used. Also it is always easier to write policy for a developing infrastructure rather than trying to retrofit it into an existing business environment.

Mitigating Liability

As you might or might not know, all business processes come with a certain amount of risk. Safeguards are placed into our business processes to mitigate this risk. A security policy takes business processes into consideration and applies best practices to protect them. This can help reduce the liability after loss of critical data.

As security and virus protection become an integral part of the evening news, law-enforcement has increased efforts into catching and prosecuting perpetrators. More and more of the courts are asked to apply our paper-based laws to the electronic frontier. Companies without policies have found they have few liability claims because the courts understand explicit policy and not the best practices. It is to the company's legal advantage to have this written down before being challenged in court.

The new economy has put a premium price on electronic information. Electronic information and the machines that store it are so integral to business processes that companies have been looking to insure these assets. As part of a process, insurance companies have been questioning the security policies and practices of the company. The first question an insurance company will ask is to see your security policy. Without a security policy, most insurance companies will not consider issuing an insurance policy. Insurance companies know that without having gone through the policy-making process, the company does not know what assets it is protecting, therefore making them too risky to insure.

Finally, a security policy that includes software development policies will help guide development of more secure systems. By setting these guidelines and standards, developers can be appropriately constrained, testers can know what to look for, and administrators understand what is required during this process. Custom development always represents a great cost and liability. By drafting and implementing software development polices and by giving developers guidelines to follow, liability can be mitigated.

After a Security Breach

Implementing policy after a security breach is like closing the barn door after the cow has escaped. Although it might seem too late, there may be cows in the barn that you can save. Never think that because it happened once it cannot happen again. Because it happened once it likely will happen again.

When developing policy after a security breach, never focus on the area broken. Although it is a concern, it is just one of many areas that should be a concern. Always

look at the whole picture—never one problem alone. This is the only way to write a comprehensive policy.

Document Compliance

Governments, government contractors, those who work for government contractors, and other businesses working in areas that involve the public sector must provide a way to ensure that their systems are safe and secure. Increasingly, governments and other customers have been demanding well-defined information security policies. Part of showing compliance is having a security policy. Even when starting new development, a security policy shows the customer that you are serious about his or her security concerns.

Government security requirements seem to change all the time. One thing that has not changed is the requirement that agencies set security policies, how the contractors follow policies, and how they work with their own policies. As more requests for proposals hit the streets, the requirements for security policies also will increase. If your company works with the government in any capacity, from contracting, to compliance, to enforcements, the presence of a security policy that can help avoid liability will be a primary concern.

Demonstrate Quality Control Processes

Along with compliance, companies also might want to demonstrate that their processes fall within quality control standards. International Standards Organization (ISO) 9001 describes a standard to demonstrate quality control in all business processes and procedures. If your company wants that type of accreditation, the policy will serve as a guideline for the implementation of a measurable security program required by quality control standards.

How Policies Should Be Developed

Before policy documents can be written, the overall goal of the policies must be determined. Is the goal to protect the company and its interactions with its customers? Or will you protect the flow of data for the system? In any case, the first step is to determine what is being protected and why it is being protected.

Policies can be written to affect hardware, software, access, people, connections, network, telecommunications, enforcement, and so on. Before you begin the writing process, determine what systems and processes are important to your company's mission. This will help you determine what and how many policies are necessary to complete your mission. After all, the goal here is to ensure that you consider all possible areas for which a policy will be required.

Define What Policies Need to Be Written

Information security policies do not have to be a single document. To make it easier, policies can be made up of many documents. Just like the organization of this book, rather than streams of statements, I divided the book up into chapters of relevant topics. So rather than trying to write one policy document, write individual documents and call them chapters of your information security policy. By doing so, they are easier to understand, easier to distribute, and easier to provide individual training with because each policy will have its own section. Smaller sections are also easier to modify and update.

How many policies should you write? I hate to answer a question with a question, but how many areas can you identify in your scope and objectives? For each system within your business scope and each subsystem within your objectives, you should define one policy document. It is all right to have a policy for email separate from one for Internet usage. It is not a problem to have a policy for anti-virus protection and a separate policy for Internet usage. A common mistake is trying to write a policy as a single document using an outline format. Unfortunately, the result is a long, unmanageable document that may never be read, let alone gain anyone's support. Figure 1.1 has sample list of policies that could be written.

Popular culture is full of examples showing that people have short attention spans. And face it, information security policies are not exciting topics. Subsequently, keeping the policies short, to the point, with clear statements, logically organized, in a cleanly designed document will give your document a better chance of being read. Do not try to overwhelm your audience.

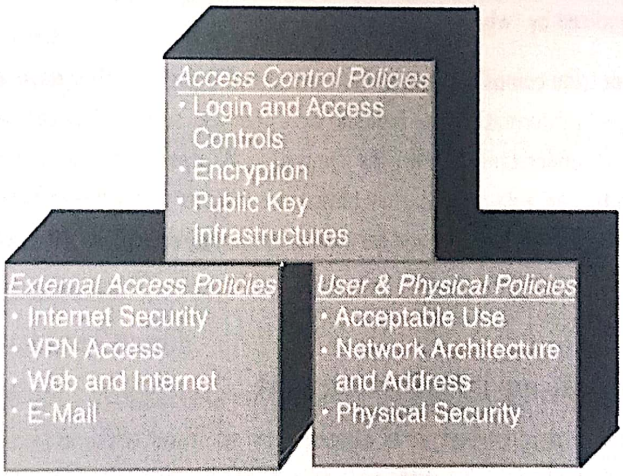

Figure 1.1 A sample list of areas that can have their own policies.

Perform a Risk Assessment/Analysis or Audit

The only way to understand your infrastructure is to perform a full risk assessment, risk analysis, or audit on the entire enterprise. By doing so, policy writers can obtain a great understanding on the reach of information technology within the organization. Although it makes the job seem ominous, it allows the authors to consider every aspect of the architecture.

As part of a risk assessment, the organization may want to do some security penetration testing. This testing should be performed both on the internal network and externally to test every known access point and to discover any unknown access points. This broad assessment provides insights necessary to understand the configuration of the network. This information should be used to determine configuration, access, and other policies. Also it will confirm how the network supports the organization's mission.

Some administrators might feel that they could explore the system, determine the risks, and inventory the enterprise themselves. Although they could possibly do an adequate job, it is always better to hire an outside company to perform this activity. The predominant reason is that they do not know your system, best practices, or other inside information that could prejudice the assessment. The outsider can come to your company and explore your systems from a hacker's point of view: Here is a potential playground, let's see where we can play! This will allow them to expose vulnerabilities, weaknesses, and other problems that you will consider when writing the policies.

> **Why Hire Outsiders to Do a Risk Assessment?**
>
> Some might feel that their own systems and security professionals could perform the risk assessment. I do not agree. While the people your company employs may be very competent, they are too intimate with operations to be able to tell a technical risk from a process risk. Outsiders do not have the same ties, so they cannot be prejudiced by "what has been."
>
> When selecting an outside company to do a risk assessment, make sure they have the resources to understand the latest security information and industry best practices so that they can provide a complete risk assessment. They must understand all the risks involved in all aspects of information technology. Because these companies do this on a daily basis, they have more insights into what to expect as they perform their tests. This objective point of view will be invaluable during your policy process.

Review, Approval, and Enforcement

As with any corporate document, it is customary to have review procedures. Information security policies are different types of documents. The review process should consider not only the technical aspects of security, but also the legal aspects of it as it relates to the organization. Prior to authoring any policies, there should be a clear understanding of the overall review process. Obviously the authors will perform the first review and then different levels of corporate review should occur. If your

company has a Chief Information Officer (CIO), that person should be on the review committee. Department heads or division heads that will be affected by a policy also should be able to review and provide comments. Finally, as much as everybody hates their involvement, the corporate attorneys also should be involved. Attorneys understand the ramifications of the policy in areas such as enforcement and what can be done to enforce the policy.

The approval process is a simple matter of the management agreeing to the final version of the document. Their approval should come after it is reviewed. However, if management fails to bless these documents, its effectiveness will be limited.

Finally, after the policy is written, approved, and administrators implement its directive, the policy must be enforced. Policies that are not enforced will be broken at will. It is the same as laws that are not enforced in society. Why go through the process of creating security policies if the provisions are being ignored? The policy must have provisions for enforcement, and these measures must be carried forth.

Summary

1. Security policies
   - Are distinct from guidelines and standards.
   - Are distinct from procedures and control.
   - Describe security in general terms; they do not describe how to implement.
2. Policies are important to
   - Assure proper implementation of control.
   - Guide product selection and development process.
   - Demonstrate management support.
   - Avoid Liability.
   - Achieve consistent and complete security, avoiding fragmented efforts.
3. Policies should be developed
   - Before security problems occur.
   - To avoid liability.
   - After a security breach.
   - To document compliance and demonstrate quality control processes (for example, ISO 9001).
4. Policies should be developed by
   - Setting the scope and objectives for the policy document.
   - Defining what policies need to be written.
   - Performing a risk assessment/analysis or EDP audit.
   - Defining effective review, approval, and enforcement procedures.

2 Determining Your Policy Needs

NOW THAT WE KNOW WHAT SECURITY policies are and have the support of management, the next step is to understand exactly what is being protected. This understanding goes beyond the hardware and software that makes up the system. It is very important to understand the business process that the technology supports. Your policy could sit on the shelf collecting dust if it prevents the company from doing business.

Identify What Is to Be Protected

In the first few pages of this book, I have repeated that the information security policies must protect the company's mission or business process. I did this because it is a common mistake to try to look at the computers and software from a technical point of view instead of why they were purchased. If you remember that computers are the tools for processing the company's intellectual property, the disks are for storing that property, and the networks are for allowing that information to flow through the various business processes, then you are well on your way to writing coherent, enforceable security policies.

Hardware and Software

Supporting those business processes are the hardware and software components that will be protected by the policies. Therefore, it is important to have a complete inventory of the system, which should include a map of the network. There are many ways to create this inventory or produce a network map. Regardless of what methods are used, you should make sure that *everything* is documented. Following is a sample list of hardware and software items that could appear on an inventory. This might not be a complete list for your specific environment; you should consider how to tailor this list for your company's purposes.

Sample Inventory List

Hardware

- CPUs
- boards
- keyboards
- terminals
- workstations
- personal computers
- printers
- disk drives
- communication lines
- terminal servers
- routers
- diagnostic equipment

Software

- source programs
- object programs
- utilities
- diagnostic programs
- operating systems
- communication programs

One way to map the network is to show how the data flows through each system. A *data flow map* can show how the flow of data supports the business process as well as highlight areas where it is important to apply security and survivability measures. In turn, that map can be used to inventory where data is stored, including databases, how it travels through the system, backups, audit, and administrative logging information.

Non-Computer Resources

Inventories, like policies, must go beyond the hardware and software. There should be a list of documentation on programs, hardware, systems, local administrative processes, and other documentation that describes any aspect of the technical business process. These documents can contain information regarding how the business works and can show areas that can be attacked. Remember, the business processes can be affected by industrial espionage as well as by hackers and disgruntled employees.

Data Flow Mapping and Survivability

Survivability is the ability to determine how a system maintains its mission and critical processes in the presence of attacks, failures, and accidents. It is based on the research performed in the CERT Coordination Center at Carnegie Mellon University (www.cert.org). Their research demonstrates that instead of using the traditional fortress-like security model, networks should be considered as unbounded, independent entities with defined communications paths and specific trust relationships.

Analyzing a system for survivability involves understanding the business requirements of the network, the architecture of the network, how it is used to satisfy those requirements, and a trade-off analysis to ensure the survivability measures also maintain the business environment. Part of the analysis and the usage requirements is the understanding of how data flows through the system. By understanding this flow, an analysis of critical processes can illustrate where resistance should be applied and demonstrates necessary limits placed on the architecture by the business requirements.

For more information on CERT's survivability research, see Appendix B, "Resources."

Similarly, the inventory should include all pre-printed forms, paper with the organization's letterhead, and other material with the organization's name used in an "official" manner. Using blank invoices and letterhead paper allows someone to impersonate a company official and use the information to steal money or even to discredit the organization. So, include those supplies in the inventory so that policies can be written to protect them as assets.

Taking Inventory of Human Resources

The most important and expensive of all resources are the human resources that operate and maintain the items inventoried. To inventory the people involved with the operations *and* usage of the systems, data, and non-computer resources will provide an insight as to what policies are necessary.

Creating an inventory of people can be as simple as a typical organizational chart of the company. This can be cumbersome, however, if you are including a thousand or even a few hundred people in one, big document. Moreover, organization charts are notoriously rigid and do not assume change or growth. The inventory, then, could include the type of job performed by a *department*, along with the level of those employees' access to the enterprise's data. For example, if the company has a large sales department, creating an organization chart with everyone's name may serve the egos of those included, but the chart becomes unmanageable. Rather, the inventory can include the "Sales Department" noting that some number, which may be unspecified, of salespeople work there.

One positive aspect of this exercise is that management can gain an understanding of who is working for the organization and in what area. As part of this process, management can see duplication in processes, identify strengths and weaknesses, and show where there might be organizational problems. This type of analysis is similar to survivability of network systems—but on a human scale. Managers should not have to be reminded to act appropriately during this process.

Identify From Whom It Is Being Protected

Defining access is an exercise in understanding how each system and network component is accessed. Your network might have a system to support network-based authentication and another supporting intranet-like services, but are all the systems accessed like this? How is data accessed among systems? By understanding how information resources are accessed, you should be able to identify on whom your policies should concentrate. Some considerations for data access are

- Authorized and unauthorized access to resources and/or information
- Unintended and/or unauthorized disclosure of information
- Outline enforcement procedures
- Bugs and user errors

Primarily, the focus will be on who can access resources and under what conditions. For example, human resource data can be accessed by authorized human resource personnel but not by the general user population. The policy might need to allow direct access of personal data but should define what "direct access" means. Of course, the policy would limit access to those who should not have this type of access as well.

After you define who can have access, a consideration needs to be made as to what enforcement mechanisms and penalties should be placed on unauthorized access. Will the organization work with law enforcement? What disciplinary action will be placed on employees who violate the policy? Legally, what can be done?

Legality of the organization's actions is very important. In this litigious society, it is important to specifically state the ramifications of violating the policy. In some states, it may be enough for the policy to say that the employee can be dismissed and "prosecuted to the fullest extent of the law." However, others may require specific language explaining the applicable laws. This is where having a lawyer on the policy-writing committee can be helpful.

This advice extends to access of the organization's systems through external means. By saying "external means" we are not limiting access to just the Internet. Access can come through Virtual Private Networks (VPNs), private networks (such as a customer network that uses Frame Relay), or modems. These access points must be defined, and policies must be created for what can and cannot be accessed from them. Because access policies are a very important basic protection to any organization, the topic will be covered fully in Chapter 5, "Authentication and Network Security."

As the software development cycle gets condensed to work within what has been called "Internet time," we all must live with bugs and user errors. These are unintentional intrusions on the secure operations of a network that can interrupt mission-critical operations. Although it is difficult to anticipate what to do in the case of failure or errors, it should be included as part of the analysis. One way to think about how to consider non-intentional problems as well as possible intrusions on the systems is to use Survivable Network Analysis Method (SNA) for analyzing network survivability. See Appendix B for pointers to the papers on the SNA Method.

Survivable Network Analysis Method

When analyzing the network for survivability using the SNA method, the first three steps are to gather the system definition, understand essential capabilities, and assess compromisable capabilities before performing the survivability analysis. These steps are essential for the analyst to understand the nature of the mission for which these systems work—thus understanding and allowing for necessary tradeoffs in design that can be important to the analysis. Using SNA, the architecture and usage scenarios are used to analyze how the network is used.

The key to SNA is that it requires the definition of two types of network usage scenarios:

1. Normal usage scenarios (NUS)
2. Intrusion usage scenarios (IUS)

NUS analysis defines how the system and components should be used under "normal" conditions. Thus anything that is not normal can be considered for intrusion analysis. IUS can be defined to understand the potential impact of a successful attack or accident. This type of analysis is very useful to understanding how the network components inter-operate.

Data Security Considerations

Everything we do with computers and networks allows the flow and usage of data. Every company, organization, and government agency is focused on the collection and use of data, regardless of their function. Even manufacturers have critical data-handling aspects of their operations that include pricing, shop floor automation, and inventory controls. The handling of the data is so important that in defining the policy needs and collecting inventories, understanding the use and structure of the data (as well as where it is stored) should be a requirement of all involved with writing security policies.

Handling of Data

How will data be handled? There are many aspects of dealing with data that must be considered when writing policies. The policies must consider how data will be handled and how to maintain the integrity and confidentiality of the data. In addition to the handling, consideration must be made to how handling that data will be audited. Remember, data is the lifeblood of your organization; you should have mechanisms to trace its life through the system.

What about using third-party data that may be confidential and proprietary? Most data sources have associated usage and auditing agreements that are included with the acquisition of that data. As part of the inventory of the organization's data, external services and other sources should be added to the inventory. The inventory also should identify who works with the data and under what conditions this data is collected and possibly disseminated.

> **Care and Handling of External Data**
>
> *External data* can be defined as any information collected, bought, or given by a source outside the company. Many times this data comes with copyright or confidentiality agreements that dictate how the information is used. Whether it is information or the source to a vendor's latest release, mechanisms must be in place to enforce the agreements by which that data is acquired and used.
>
> One trap is the collection of information from public data sources that are incorporated into other works. It is easy for employees to cut-and-paste information from web sites and other sources into internal documents. While this is legal under fair-use standards, the employee should provide proper attribution, especially if the information is quoted verbatim. Yes, they should know better. However, this should be reinforced by the policy and be included in the security awareness program.

Just as other organizations share information with you, you also might want to share information with them. Whether it is because of a partnership agreement or other business relationships, mechanisms must be in place to protect the disseminated data or technology transfers as intellectual property. When writing these policies, some of the considerations for disseminating intellectual property are

- Use of company information for non-business purposes
- Definition of intellectual property-handling requirements
- Transfer of information to a third party:
  1. Confidentiality agreements
  2. Full-disclosure records
- Protection of disclosed data

It is difficult to anticipate how the business circumstances define what can be disclosed and how, but the policy should include a review of these processes. One way to understand their impact on policy is to understand how current agreements are handled. As part of the inventory process, any attorneys working on the committee can gather these agreements and notes on current discussions. Using this information, policies can be written as guidelines to protect the company in information and technology transfers.

A common omission to these policies is the requirement to classify information. One common method is the use of security labels. Although the use of security labels is not consistent across all operating systems, databases, and software programs, policy writers should consider how to mark data for their level of security. There are many circumstances where this is necessary. In particular, personnel or health care information are prime candidates for security labeling.

Personal and Personnel Data

During the course of business, an organization can collect personal and personnel information in many ways. Those involved in e-commerce may collect information from access to their web site. Companies that sell products and services can collect

customer data through order/entry or customer service calls. Even sales calls or potential customer inquiries can yield personal information about a person or a company. Regardless of how this data is acquired, policy statements should be created for everyone to understand how the data is used.

Privacy Polices and Public Policy in the United States

As I write this, public policy makers in Washington are discussing the practice of collection and handling of personal data during the normal business cycle. In recent news, the Federal Trade Commission (FTC) has recommended that congress pass laws requiring companies to disclose how they handle information they collect from access to web sites. This came after finding that many web sites do not have posted privacy policies or policies that are followed.

Currently, the FTC privacy guidelines are merely guidelines and not part of public law. At the FTC's request, Congress is looking into the issue. As with many controversial issues, predicting what Congress will do can be a full-time job.

One thing to consider when beginning this process is how your organization operates outside your home country. U.S. companies doing business in Europe, for example, might be subject to strict privacy laws in Germany and Scandinavia. Although these policies may not be popular within your organization, it will help when working outside the United States. For further information, see Appendix B.

When considering privacy policies, the observance of privacy must be defined so that the organization not only observes the employee's or customer's right to privacy, but also that the employee observes the organization's right to privacy. Policies can be written to state that private, proprietary, and other similar information should not be disclosed without prior consent.

Privacy policies are not easy to define. Because policies are guidelines and not procedures, some organizations prefer to define exactly what is protected in procedures documents. One of the best ways to determine how to partition this is to gather what should be included in privacy policies and look for one or a short number of common statements. Those statements become the policy. How the data is handled then becomes a matter of procedure.

COTS Licensing

Policies for Commercial Off-The-Shelf (COTS) software licensing must consider that in most cases, the organization does not own the software or the data governed by those licenses. COTS licenses allow you to use the software under specific restrictions. This means that COTS policies should be based on following those licenses.

The software industry has been increasing their licensing enforcement procedures through the Business Software Alliance (BSA) industry consortium. Working from tips that usually come from disgruntled employees, the BSA audits and reports on the licensing status to the owner of the software. After an investigation, the BSA supports the company in filing breach of contract lawsuits against offending companies.

Strong COTS policies should include the periodic review of licensing agreements, guidelines for acquisition and evidence of software licenses, and records of registration of products with vendors. Additionally, policies on copying should be included and should mandate strict management and accountability of those resources.

I have heard one common theme when discussing COTS policies with others: Software licenses are assets and should be treated as such. This is not a far-fetched idea. These licenses are tangible assets that have value, can be counted, and can be depreciated like the machinery on the shop floor. This will please the Chief Financial Official if he or she has not considered the value of software to determine the amount spent on property, plant, and materials.

Backups, Archival Storage, and Disposal of Data

Policies about the handling of data backed up to external sites or off-site media is as important as for online accessible information. Backup data can contain financial information, a history of customer interaction, and even copies of current business. If the data is not to be kept, what would happen if the competition were able to obtain and analyze that information? What if they found data that should have been discarded? Backup policies, therefore, must reflect on the processes themselves, cover how the data is archived, and provide direction for what to do when data is to be discarded.

Backup Considerations

Why does your organization back up information from its computers? Is it to recover from system crashes? Preserve critical data? Does your organization want to keep a snapshot of system software? How often are these backups made? Are they made daily, weekly, or monthly? And how do you do them? How often is this process reviewed and verified?

All good questions, but how do the *answers* to these questions enable the backups to support the recovery-critical business processes after a failure? An inventory of the business process also should include the recovery processes and the information processing that is necessary to support them. That knowledge will help determine how to answer those questions and set policy.

A common mistake in setting backup policies is to mandate the special options available in the software package the company is using. When determining how backups support the business process, policy writers should try to confine the document to describe what should be done and avoid mandating special options. The following are a few questions to be considered when analyzing backup policies:

- Which data will be backed up?
  - Only user data?
  - The whole system?
  - Entire database or journal files?

- How often should backups be made?
- How are backups to be performed: automated, multiple copies, or media?
- How often are the backup procedures reviewed?
- Will you use off-site or on-site storage for backup media? How will you secure the on-site storage area?
- Who will be allowed to perform the backups?
  - Who will be allowed to have access to the restorable data?
  - Who will be allowed to restore that data?

Archival Storage of Backups

For some, the last consideration of handling backups is how to store the media or safeguard the data. As part of the audit and inventory of operations, special note should be made of current practice. If the current practice does not safeguard data, then here is your chance to make the safeguards policy.

When considering backup archiving, one of the first concerns might be whether the media will be stored on-site or off-site. Some organizations have storage vaults for storing tapes and disks. For them, policies for on-site storage should be sufficient. Otherwise, understanding the current and best practices can help create a workable policy.

Several years ago, I retrieved a tape from the vault where my company stored its backup tapes. The vault was climate controlled and specially designed to store up to 6 years of 9-track tapes. The tape I chose was created only 18 months earlier. I mounted the tape on the local drive and tried to read its contents. After spinning for only a few hundred feet, the driver printed an error and the system refused to read the tape.

After trying several tapes, I looked at the service log and found that the system's field engineer adjusted the drive heads after someone complained about not being able to read a tape sent by a client. Although the adjustment was necessary, tapes for the three months prior to the repair date were unreadable. Had we known this would be a problem, there would have been a chance to recover the data. Unfortunately, there was not a policy on handling the data or checking the backup. Since then, I have insisted on a clause to include testing the archive.

That brings me to another point: Why was the vault nearly filled with six years of archives? Did we need six years of data? We did, but does the data that your organization stores require it to be saved for that long? If not, then how long? In cases where the retention time is longer than the life of the media (the typical life of magnetic tape can last an average of two years), maybe you should consider a policy that specifies *write-once media*. Notice that I said "write-once media." Remember the lesson learned in Chapter 1, "What Information Security Policies Are": By considering a policy with general wording, you allow the people creating the archives to determine the best

technology to use. This allows for the use of new technologies that may allow the data to be archived longer than current options.

Disposing of Data

"Dumpster diving" is a common practice when those practicing industrial espionage seek information on their target. A colleague who used to work in this area would surprise me with stories about what some companies throw out. One day, he hit the jackpot. He collected more than two dozen cartridge tapes from the dumpster of a competitor that contained information that the company should have made sure was kept confidential.

How does your organization dispose of data? If you are throwing away tapes without erasing them, then the dumpster divers will surely find your company's secrets. Determining how the data is disposed of is as important as determining what data to discard. Make sure that this policy specifies how to erase or discard the data *and* that it defines a requirement for verifying that the data can no longer be read.

One way to ensure that this policy will be carried out is to assign the responsibility to discard the data to one person and the verification to another. The policy should mandate that a regular schedule or a rigid procedure be followed so that both responsible parties can verify that those who should not see it could not access the data.

Intellectual Property Rights and Policies

Every organization, regardless of its function, has intellectual property that it protects from disclosure. Even if the organization does not have information security policies, it probably has rules and procedures for safeguarding its intellectual property. Not every organization puts the same emphasis on this property, however. For example, a company that is a price differentiator will guard its manufacturing process to prevent its competitors from discovering how they can keep their prices down.

Intellectual property policies are probably the most difficult for most information security professionals to write. Not only are these policies tied to the business process, but the body of law covering intellectual property covers volumes and can differ between states and countries. When planning and writing these policies, it is highly advisable to consult an attorney whose specialty is in this area. In the preliminary stages of planning, the following are a *few* considerations for intellectual property policies:

- *Who owns the rights to the intellectual property?* Assignment of patent, copyright and other intellectual properly rights should be stated in a policy, whether it is within the information security, corporate, or employee manuals. Having this spelled out in a coherent policy can provide a solid basis to protect the company's property in court if that should become necessary.
- *What are the rights to programs and documentation?* After ownership of the intellectual property has been established, what rights do employees have with the

programs, processes, and documentation? While an employee might have access to the manual that describes the latest business process or the new re-engineering plans, the policy may prevent them from taking that manual out of the plant or talking about that information with others. And the policies can define who those "others" are. In fact, some policies require that procedures define access rights to the document and processes:

- *All sources of information should have an attribution.* Graphical User Interfaces (GUIs) and the World Wide Web make it easy to gather then construct information by copying from the browser window into the window running the editor or word-processing program. Sometimes it is too easy. Making copies of someone else's work and incorporating it into your own without attribution is plagiarism. Yes, you can use small sections under the "fair use" laws, but these sections must be attributed to the original author. The policy statement can say that the company will not tolerate plagiarism while leaving attribution standards to style guidelines.
- *Labeling for paternity rights to intellectual property.* If the work is covered under patents, copyrights, or nondisclosure, it must be labeled with the appropriate information. Without quoting the cases, several have gone against the owners of intellectual property when they did not make their rights known nor took measures to protect those rights. Some companies mandate that all printed material contain the words "Company Confidential" on all pages. Labels must be conspicuous and clearly state ownership. Your attorney who specializes in intellectual property law can help in this area.

When working with intellectual property, whether it belongs to your organization or you acquired it from someone else, make sure you know your rights under the agreement. For example, many software programs allow the user to create one copy for backup purposes but not allow more than one copy to be running at any given time. As for written works, there are still "fair use" laws that allow a limited number of copies for personal use. Once the usage is allotted for business purposes, you should talk with your attorney about what is and is not allowed.

Technical People and Intellectual Property

There are many urban legends regarding the handling and protection of intellectual property. One of my favorites says that a way to copyright a work without filing the necessary papers is to mail ten copies to yourself. The postmark on the unopened envelopes would be enough to establish the date and location of the work.

Technical people tend to work hard on an idea, and then they take these legends seriously in an attempt to save money. Later, they find that these schemes offer no protection. Intellectual property is such a complex subject that myths and legends should not be your guide in protecting your organization's most important asset. Instead, talk with an attorney who specializes in this area. The attorney will tell you that all you've done with those ten envelopes is added money to the coffers of the postal service.

Incident Response and Forensics

I think I subscribe to every information security mailing list. These lists give me varying levels of details on the bugs and other vulnerabilities that can cause security problems within systems or networks. Some are general while others are run by manufacturers and cater to users of that vendor's product. Most contain information submitted by users while the rest comes from the manufacturer. I know that the number of mailing lists I am on is overkill to most administrators, but the point is that as I work with my clients, I am kept up to date on the latest information.

Yet one day, you are sitting in your cubicle, and you discover a security hole that once publicized, if attacked by a hacker or a disgruntled employee, could bring down the organization's network. Rather than trying to bury the information, you try to publicize it.

Some people feel that incident reporting is an important service to the Internet community. So they go out of their way to report problems they found. Many of these organizations have a policy for incident reporting. You can send the information to over 30 different incident response organizations. To help these services, your organization could have a policy to work with one (or a few) incident response team(s) through one point of contact. By limiting the responsibility to one person, or a backup, information can be efficiently transmitted from a single, authoritative source, and it will not be lost in a sea of messages that might even conflict.

> **The CERT Coordination Center**
>
> The granddaddy of all the incident response teams is the CERT Coordination Center (CERT/CC) at Carnegie Mellon University in Pittsburgh. Founded as the Computer Emergency Response Team in cooperation with the Department of Defense following the Internet Worm in 1988, CERT/CC collects information about security incidents and investigates whether or not it is a problem that should be publicly disseminated. Although CERT/CC's methods are considered controversial, they do provide a valuable service to the community. CERT/CC is not the only incident reporting service. Appendix B provides a list of a few others.

Incident Response Strategies

On the other end of incident handling is incident response. Incident response is necessary when unauthorized access of your network is detected; when a response team contacts your organization to say that problems exist, and that they appear to be coming for your organization's computers; or when someone reports to a public service that a problem was found in the operating system or support software that your organization runs.

Like incident reporting, incident response policies should have one point of contact. That person should be responsible for collecting these reports and preparing a response to them, regardless of from whom they come. In fact, the contact person should be able to determine if an incident report is applicable to the organization. The policy could give this person the power to do whatever is necessary to solve any problems

arising from these reports or provide the ability to draw on others necessary to diagnose the problem.

Working with vendor-supported response teams is similar to working with independent services, except the vendor may contractually require your organization to choose a particular point of contact. For example, your organization might want the security officer to handle incident responses. Your vendor might want to bypass this person to work with system administrators. Allowing this requires only a minor adjustment in policy and can be written in a way to allow for working with vendor teams.

Computer Crime

As I write this, I am looking at three different guidelines for prosecuting people under different attempts at defining what is a computer crime. Each guideline tries to tie the local jurisdiction's case law (the decision and opinions made by the courts) to the written law. The only consistent theme is the inconsistency of their requirements.

Understanding what is a computer crime differs between jurisdictions. Even in the United States, each of the federal court circuits may have different interpretations of the same law. If you are a company in New York, the rules may not be applied the same to your office in Silicon Valley. The key to understanding what is allowed in your area is to make an appointment to speak with the district attorney, attorney general, or solicitor that you would work with. They know the judges and the standards of evidence necessary to successfully try a case.

However, writing a policy saying that the company will work and report all criminal activity may not be in the company's best interest. Take the story of the bank whose systems were infiltrated by hackers who stole nearly $11 million! That bank initially chose not to report the incident to any law enforcement authority fearing negative publicity. With billions of dollars in assets, it was easy to write off $11 million in "lost" funds.

One day, the bank had to report the loss in response to another lawsuit. When the press found out about how this bank lost $11 million, the negative publicity was enough to affect the price of their stock and garner additional scrutiny from federal regulators. The end result was a public relations problem, which costs.

Determining what to report and under what considerations is not something to take lightly. Policies in this area must be discussed among executive management, who must bear the burden of the decision should something happen. On the other hand, requesting that management make the decision about the appropriate policy forces them to consider security policies. How they answer will tell you how seriously they are taking these efforts. At this stage of policy writing, it is good to know how much support really exists.

Summary

This chapter discussed the need to understand exactly what is being protected. This understanding goes beyond the hardware and software that makes up the system but integrates the business process into the preparation process. Your ability to support your policy decisions will determine the success of the document.

1. Identify what is to be protected:
   - *Hardware.* CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, and routers.
   - *Software.* Source programs, object programs, utilities, diagnostic programs, operating systems, and communication programs.
   - *Data.* During execution, stored online, archived offline, backups, audit logs, databases, or in transit over communication media.
   - *Documentation.* On programs, hardware, systems, and local administrative procedures.
   - *Supplies.* Paper, forms, ribbons, and magnetic media.
2. Identify from whom it is being protected:
   - Unauthorized access to resources and/or information
   - Unintended and/or unauthorized disclosure of information
   - Bugs and user errors
3. Data security considerations:
   - Handling of data (integrity and confidentiality)
   - Handling of third-party confidential and proprietary information (who's allowed and under what conditions)
   - Protection of disclosed data (confidentiality agreements and full-disclosure records)
   - Personal and personnel data (rights to privacy and disclosure policies)
   - COTS licensing policies (periodic review, registration, evidence of compliance, and copying)
4. Backups, archival storage, and disposal of data:
   - *Backups.* What, when, how, how often, and how often reviewed.
   - *Archival storage of backups.* On-site storage versus off-site, protection of archive, documentation, testing, retention period.
   - *Disposal of data.* Who is responsible and how it is verified.
5. Intellectual property policies:
   - Information as an important company asset
   - Assignment of patent, copyright, and other intellectual property rights

- Attribution of sources for information
- Labeling for paternity rights to intellectual property
- Protection of intellectual property rights (notices and due diligence)

6. Incident response and forensics:
   - Incident reporting and response strategies
   - Determining who has this responsibility
   - Working with industry and vendor response teams
7. Computer crime:
   - Understanding that a computer crime really is only considered such according to law enforcement
   - Determining what to report and under what considerations
   - Working with law enforcement

3

Information Security Responsibilities

IF YOU ARE READING THIS BOOK IN chapter order, you probably want to start writing the policies. However, before you start to write your policy documents, you should really have a clear definition of the roles and responsibilities of the individuals in the organization with respect to security. As we have discussed in the first two chapters, management support is crucial for a successful information security program. Along with its support should come responsibility to the ongoing maintenance of this program. This chapter will emphasize the responsibilities of management and the roles of those who must provide front-line enforcement. The understanding of these groups is necessary for a successful security program. The chapter ends by discussing awareness training and support.

Management Responsibility

Management's responsibility goes beyond the basics of support. It is not enough just to bless the information security program; management must own up to the program by becoming a part of the process. Becoming part of the process is showing leadership in the same manner as it does in other aspects of the organization.

When I tell this to people in management, I get a reaction of shock or horror. After all, they are not trained in technology or information security. I explain that they do not have to understand how it works, but they need to be involved to ensure that the

business processes are protected and not hindered by security decisions. Management has specific goals for the organization, and most security and information system professionals are not in the position to understand or appreciate these nuances. This is not a knock against management or technical people, but years of misunderstandings have created animosity between the two groups.

Both groups should understand that security is not something that can be wrapped in a package and bought off the shelf. It is a goal that both parties strive to maintain. It comes after the analysis of risks, costs, and the requirements to ensure that information is not too secure to access. Management is responsible for doing the analysis and conveying this to the technical people responsible for implementing these policies.

Information Security Management Committee

One of the ways to help bridge the divide between the two groups is to create an *Information Security Management Committee*. This committee will be responsible for reviewing changes in the business plan and determining how the security policies should support those changes. Another purpose of this committee could be to review the procedures, assuring that they comply with the policies as well as requests for exemptions to the policy.

To make this committee a success, it should be made up of a diverse population and be similar in makeup to the group that authored the policy document. However, the difference is that this committee should consist exclusively of management representatives who will understand the implication of the policy from both the business and technical perspectives. This assumes that technical management understands the issues and has access to information to help make good decisions on security issues. Not every member needs to be executive-level management, but it would be a good idea for the committee to be represented by someone from the executive suite.

Information Ownership

One of the more difficult tasks for management, or even the management committee, is to assign responsibility for information assets or controls—also called *information ownership*. By designating an owner, that person becomes responsible for maintaining the information asset according to policy.

Information ownership is not an easy concept for many people. In the traditional security model, data and controls are kept on the servers under the watchful eye of an administrator or administrators. That administrator, then, must understand how that system is used and how to set access controls. Problems occur when the administrator has to manage a diverse set of controls for many different servers, databases, data stores, or just "assets." To keep a sense of order, the administrator makes policy implementation decisions based on the least common denominator of everyone those systems serve.

In this "one-size-fits-all" scenario, the administrator sets the classification, sensitivity, and access controls for the data to be consistent with the assessment of his or her job. There is no guarantee that these attributes will be compatible with the policy as it applies to every person that accesses the information. Conflicts can occur between users requiring access to information and administrators who have made the wrong assumptions.

An alternative method would be to assign ownership of the data and controls. The owner would be responsible for defining access to the data and determining how the controls are to be set. The owner would work with a security and/or systems administrator to manage the information assets. The owner would determine the sensitivity and classification instead of leaving it up to the administrator. This result would be the managing of assets to satisfy the needs of the owner.

The owner would be responsible for handling variances from generally accepted practices. If the request for information requires controls that are inconsistent with policy, the owner is then responsible for the necessary changes and subsequent repercussions. Some organizations require information owners to request variances in writing and sign a disclaimer taking full responsibility for any potential problems. Because many do not want to take the career risk involved with this responsibility, requests for variances are rare.

The downside to information ownership is that the owner is responsible for maintaining controls in a manner consistent with the security policy. Further, some owners may feel that the requirement to take full responsibility is not fair or not worth the risk, thus they do not follow procedures and ignore policy. From the beginning, the owner must understand the impact of the responsibility he or she has to the information. The only way to mitigate this problem is through proper security awareness training, support from management, and consistent and stringent enforcement.

Another problem with information ownership is that it only really works well in diverse organizations where data can be partitioned among potential owners. I have not seen this work well in marketing organizations or in others where data is thoroughly integrated in the environment. Information ownership also can be a problem in smaller organizations where there may not be enough people to support this concept. One company I worked with that tried information ownership made all 20 employees co-owners of the data. Although this was done as a morale booster, it also helped maintain the integrity of the data.

If your organization is not comfortable with the concept of information ownership, you might want to adjust your policies to create committees of responsibility. By creating small committees, they can do the same thing owners would do, but no single person would have to accept responsibility. Rather, the entire committee becomes the responsible party. This creates a situation with additional checks and balances when variances are requested.

Assigning Information Ownership

The first rule of assigning information ownership is to make stakeholders the owner of their own data. Simply, the owner of financial data should be someone under the Chief Financial Officer. This is not an easy process. The point is not to create catch-all departments, unless it fits the business process. This also means that the Information Systems Department must not be the owner of information except that which is needed for operations such as configuration, user identification information, domain name service (DNS), and the like.

As part of the process, you should talk to the stakeholders. By discussing information ownership with those directly involved, you can understand their concerns. You might even get ideas regarding how to assign or structure ownership.

Ownership should be assigned based on a high-level inventory of information assets. You can use the same inventory as created during the preliminary processes (described in Chapter 1, "What Information Security Policies Are"). I suggest the high-level list be used so that there are not too many information owners. It may require additional analysis into who should own what information, but limiting it to a few key players will help manage the process. Then, each major information type should have a designated custodian assigned from the inventory.

Security Responsibilities for Information Ownership

If your organization decides to assign information ownership, you have to consider what responsibilities these owners have. Guidelines written into the policy should define the specific controls information owners are allowed. By "specific," I mean what controls they can work with, not how those controls are implemented. These policy statements also can discuss the administration of the access controls in terms of the parameters they are allowed to administer.

The most important responsibility given the information owner is the granting and revoking of access to the company's information. As you begin to draft policies, those dealing with the access of information should include how these policies affect the information owner. Further, access policies also should consider recovery capabilities for the data and the access control processes. For example, the policy can mandate that

- If the information owner is not available, the owner should designate someone to act on his or her behalf.
- Passwords used in management of the information are also held in a password or key escrow so that they can be accessed should something happen to the owner.
- There are mechanisms to override the information owner.

Remember, the mechanisms you are considering are policies. Avoid the temptation to define the procedures information owners will follow.

Information Security Compliance Plans

When discussing management's responsibility and compliance, you should concentrate on how management should respond to enforcement as well as when policies are broken. These plans go beyond the issue of management support. These discussions should center on the roles management should play in the information security arena.

When it comes time for awareness training, management's sessions are exclusive and abbreviated compared to what everyone else must go through. Rather than separate management, see if you can integrate management into the security plan. Make management an active participant. While it is not necessary to have an executive actively review log files or site-inspect facilities (although they might be a good ideas), they should be involved with settling disputes and counseling employees that violate policy. Should a problem require the assistance of law enforcement, members of management should be on hand as an active participant in the investigation.

This may be tough to sell to nontechnical management. Even in the move to automate business processes, management that does not understand technology tends to hide behind their technical people or consultants. Although information security is not really a technical issue, it is seen as such. One way to include them in the process is to have them own the processes, just as other managers own the data. By making them the owners of the processes, it will give them a sense of responsibility, which will not allow them to wilt behind their desks and management committees. For that sector of management whose ego needs a boost, giving them responsibility will add to it.

Role of the Information Security Department

The Information Security Department is responsible for implementing and maintaining organization-wide information security policies, standards, guidelines, and procedures. They should provide security awareness education and ensure that everyone knows his or her role in maintaining security. Simply, the Information Security Department provides the mechanisms that support the security program outlined by the policy.

This department must be able to strike a balance between education and enforcement (see the "Security Awareness Education" section that follows). It will be difficult to find this balance. The policies guiding this group should be written down to ensure that these roles are clearly defined. They should be viewed as a partner in the business process. If implemented as an enforcement-only group, the Information Security Department will be feared. Fear can elicit adverse reactions to its real purpose, which can undermine the purpose of these policies.

Chapter 12, "Compliance and Enforcement," as its name makes obvious, is dedicated to compliance and enforcement, an integral component of security awareness education. Read ahead if you need more information about the role of training before continuing with the policy-writing process.

Security Awareness Education

The importance of security awareness training and education cannot be overstated. By taking the policy seriously and teaching all of the stakeholders about their role in maintaining it, they will embrace the policy as an integral part of their jobs. This is not easy. One problem is that over the last decade, industry-leading companies have not demonstrated a concern for security in their products. The results are products that have insufficient security measures installed into environments that further weaken the information security program. The dichotomy can be confusing.

Security awareness training requires clear communication. One thing you might consider for your organization is hiring a technically competent communicator for the Security Department. This person would do the training, educate the department to the concerns of its users, and act as a liaison between users and the department. Having someone who can communicate will help raise the confidence level users should have for the department.

Use of Consultants for Information Security

Outsourcing has been a staple of the computing industry since companies offered time-sharing services on expensive mainframe systems. Today's outsourcing environment can provide information processing services for every aspect of the organization, including information security.

There are some serious concerns in using consultants or outsourced services for information security. When determining policy goals for the outsourced environment, a few things should be considered:

- *Work with in-house Information Security Department.* It is highly recommended, even if information security is outsourced or consultants are used, that the organization maintain a small department—even if it consists of only one security expert. Information security is something that requires a trust relationship among the users of the information and those enforcing the policy. It may be difficult for some to trust an outside source.
- *Set clear guidelines.* As with any outsourcing or contractor agreements, clear guidelines on the roles and responsibilities must be defined for these outsiders. It may not be in the organization's best interest to provide these outsiders open access to the information assets. Therefore, a clear *statement of work (SOW)* should be included as part of every outsource information security agreement that clearly outlines guidelines. The SOW should not be part of the policy documents, but its guidelines should be stated.
- *Determining responsibility.* Another aspect of the SOW should be to determine the responsibility of the outsourcing or contractor in the organization's information security environment. Policy should include the responsibility of anyone working as part of this environment.

Other Information Security Roles

For any information security program to be successful, it must be integrated into every aspect of the environment. Integration must include statement of work and responsibilities within the business environment, job descriptions, and how these will be audited and monitored.

Integrating Information Security into the Business Process

A primary task in assigning roles in the information security process is how information security integrates into the business environment. As part of that integration, jobs that support security through the processes should be defined. For example, one way to do this is to define a separation of duties and control over company assets by coordinating efforts with everyone, including owners of data and facilities. By having these defined as part of the business process, there is no ambiguity as to who is responsible and when.

Another role to consider is how security is administered throughout the organization. A typical environment should have a central information security management group. The central group is in charge of the monitoring and enforcement of the policy and procedures. Consider an approach from unbounded systems (see the description in Chapter 2, "Determining Your Policy Needs") where the central security management group designates security administrators for multi-user and multi-departmental systems. Each department then supplies its own security officer or liaison who will help maintain the security program for the department. This has the effect of putting enforcement closer to the users, sort of like police departments returning to the concept of the cop walking the beat.

The closer placement of security enforcement will help with the control of real-time connections with third parties. Not only do threats exist from employees, but customers, vendors, and anyone else with connection to the organization's information assets can violate policy. These liaisons can be responsible for educating these outsiders as well as monitoring and providing enforcement. This works in smaller organizations. Many compartmentalize themselves into "departments" that can participate by assigning one person as a security liaison, especially when working with people outside the organization.

This, however, is not a perfect solution. Some people who work in this environment for an extended period might find ways to abuse the system and exploit it, for whatever reason. One way to combat this is not to allow a person to be the security liaison for more than a short period of time, one or two years for example. At the end of the term, they pass the job to someone else. Another way is to set a policy of checks and balances. One manageable process is the organization's procurement system. Even though most purchases have an approval process, many times those approvals are passed along and paid without further notice. Instead, a security liaison within the Accounting Department should look for anomalies in purchases and orders shipped.

Those who do forensic accounting tell me it is not an easy job and is a job that cannot be done by just anyone. The forensic accountant must know the business process, customers, vendors, new business, old business, and how the money flows through the organizational machine. Using this knowledge, the forensic accountant can read invoices or purchase orders and determine if there are unusual purchases or sales that may indicate an internal problem.

The final area that should have a role in the information security process is the software development cycle. Whether software is developed internally or by contractors or if the organization purchases Commercial Off-The-Shelf (COTS) products, the goal should be to build secure systems wherein errors or manipulations can be trapped. Policy for coding and testing standards also can assist in the quality assurance process. Moreover, using a paradigm such as survivability (as described in Chapter 2) can form a basis for designing software that does not cause or reveal problems when deployed.

Individual Information Security Roles

One way to ensure that every current and future employee or user knows that security is part of his or her job function is to make it part of each job description. Spelling out the security function or expectations within the job description demonstrates the commitment to information security as well as emphasizes that it is part of the job. After it is made part of the job description, it becomes something that can be considered in performance evaluations.

Outside contractors, vendors, or other people that provide external services directly on the company's network should include similar language within their SOWs. As with employees, this reinforces the company's commitment as well as makes the contractors' or vendors' adherence to the organization's security requirements a factor in their quality-of-service evaluations.

Auditing and Monitoring

Auditing and monitoring are important for enforcement and compliance of security. However, if this is not a role within the business process, there is a danger that it may never be done. Think of this process as the quality control of your information security program. That way, the roles required to provide internal audit of information system controls will be a natural occurrence and not considered a surprise attack.

In later chapters, we will talk about the independent review process. For now, however, consider it a role of someone to arrange and supervise this review.

Understanding Security Management and Law Enforcement

As I write this, it is being reported that Microsoft was allegedly hacked by overseas intruders. News reports are saying that the hackers supposedly used viruses to plant

Trojan Horse programs, hackers were able to download Microsoft's proprietary source code. There have been other famous intrusions and manhunts for the perpetrators. Unfortunately, with the exception of a few high profile cases, most of the electronic trespassers do not get caught.

Compared to other areas of law enforcement, computer crime and information forensics are in their infancy. Like in the days of the Old West, the police today must face the problems that arise from any new experience. First, there are jurisdictional concerns. The nature of the Internet, multi-national corporations, and the growth in worldwide telecommuting blurs the borders between states, provinces, countries, and continents. If they ever find the perpetrators of the Microsoft break-in and that person is from overseas, under whose laws will they be prosecuted?

Whose Jurisdiction Was It?

In 1999, computer students in the Philippines wrote a virus that attacked a popular commercial mail program that caused millions of dollars in estimated damages from the cleanup. When the experts traced the messages to the Philippines, the U.S. Justice Department worked with Philippine officials to have the hackers arrested. Justice Department officials claimed that they had jurisdiction over the alleged crimes even though the perpetrators were Philippine citizens on home soil. Philippine officials could not arrest them because there were no laws covering their alleged charges.

The United States does have an extradition treaty with the Philippines, but how effective is it to bring these hackers to the United States to stand trial? Thus far, the hackers have been charged with misdemeanors and are still in the Philippines. It will take a long time for diplomats to understand the impact of computer crime and the treaties that are necessary to protect national and international infrastructures.

Another problem is understanding how computers impact the law. Although there are a number of laws covering computer crime, they are still written to conform to a paper-based world. Even though there are examples of how the laws covered the telephone as it evolved, legislators have yet to learn from those experiences, leaving us with a variety of laws.

I am telling you this not to discourage you from working with law enforcement when a crime is committed. On the contrary, I want to prepare you for what will seem like an uphill battle to bring an alleged criminal to justice. The first thing you can do is to know the law. I understand that administrators and security people are not trained in the law, but there are many resources that can help you understand what kind of protections the law provides (references can be found in Appendix B, "Resources").

Another important aspect of the law is understanding what is required to prosecute crimes in your jurisdiction. Not only are the laws different across borders, but in the United States, applications of federal laws differ between the districts of the U.S. Courts. Unfortunately, the federal district courts are like fiefdoms; precedents in one do not affect another until ruled on by the Supreme Court. This means you have to understand what the rules are for the district where your case will be handled.

One of the best ways to understand what it will take is to ask your local law enforcement officials. It is very common for physical security professionals to discuss their plans with police and prosecutors. However, with the exception of the FBI through the National Infrastructure Protection Center (NIPC), you may not get cooperation because they may not understand how to help.

Do We Need an NIPC?

The National Infrastructure Protection Center was formed in 1998 by a presidential directive to serve as a resource from which law enforcement could gain knowledge on how to protect the growing critical information infrastructures. Although it is a noble concept, there are some who believe that the FBI should not collect and keep this information. Some have even harked back to the days of J. Edgar Hoover keeping files on alleged subversives. Should the FBI be involved with collecting this data?

Although it has stumbled a bit, the NIPC has provided a lot of good information to law enforcement. The NIPC's InfraGuard program is designed to bridge the public and private sector to protect information resources. Its success will depend on the cooperation it receives from industry. To learn more about the NIPC, visit its web site at `www.nipc.gov`.

The primary area of focus after a crime has been committed is the handling of evidence. As part of your preplanning, learn the rules of evidence. The rules of evidence are the guidelines prosecutors must follow to legally use evidence in court. Use the guidelines to outline policy for handling data, systems, networks, and log files after a crime has occurred. Expand this into clear procedures to accompany the policy to make sure evidence is properly protected. After all, without evidence a prosecutor can use, there can be no case, and the criminals remain free.

Information Security Awareness Training and Support

After the policies are written, there must be communication among the writers, management, and everyone in the organization so that all understand the policies and impact. In this final step of the planning process, the planning for training should be considered. It is reasonable to mandate that training be required for anyone with access to company computers and networks. Human Resources should have complete records, including information on training courses required and taken as well as all signed documents showing acceptance of defined corporate policies.

Management should not only set aside time for training; they should *encourage* it. One company I was involved with mandated training during specific time periods; and unless employees were involved with a client or ill, they were required to attend. The policy allowed the employee to be suspended without pay until he or she attended the

course or watched it on videotape. You might not want to go to this extreme, but it is a good way to get 100-percent compliance.

Remember, you are writing many policies and customizing them to your environment. This means that you cannot plan on a "one-size-fits-all" training program. Plan on customizing training as it relates to the contents of the policy. Also understand that everyone does not have to be trained in all areas of the policy—Help Desk personnel, for example, do not need to be trained in software development security policies. As you plan your training policies and programs, keep this in mind to ensure that each aspect is properly covered.

Summary

Management support is crucial for a successful information security program. Along with its support is a responsibility to the ongoing maintenance of this program. We emphasize the responsibilities of management and the roles of those who must provide enforcement. To have a successful security program, these groups must have a good understanding of their function and be willing to take action. The level of compliance measures this success. Compliance can only happen if everyone knows about the policies through a comprehensive training and awareness program.

1. Management responsibility:
   - Participate and support an Information Security Management Committee.
   - Information ownership includes assignment of responsibility for information asset controls; someone is the designated owner, and the owner determines sensitivity and classification, including handling variances from generally accepted practices.
   - Devise information security compliance plans for management.
2. Role of the Information Security Department:
   - Policies should state that the Information Security Department is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures.
   - This department is responsible for education, enforcement, and protection.
   - In outsourcing or use of consultants for information security, set guidelines determining responsibility to work with the in-house Information Security Department.
3. Other information security roles:
   - Regarding the integration of information security into the business process, define the separation of duties and control over company assets, coordinating efforts with everyone, including owners of data and facilities.

Designate a security administrator for all multi-user systems while specifying that each department should have an information security liaison.

- Determine the security responsibilities for real-time connection with third parties.
- Make provision for a forensic review of invoices for abnormal purchases or sales.

- Place information security responsibilities in job descriptions and in third-party contracts, and consider them in performance evaluations of both.
- Regarding auditing and monitoring, the internal audit of information systems controls is a key role integrated into the business process.

4. Information ownership and custodial responsibilities:
   - In assigning information ownership, the Information Systems Department must not be the owner of information except that which is needed for operations. Ownership should be made using a high-level inventory of information assets. There should be at least one designated custodian required for all major information types.
   - As part of the security responsibilities of information ownership, define allowed controls and how those controls will be administered. These controls should have guidelines for granting and revoking access to the company's information and provide recovery capabilities.
5. Understanding security management and law enforcement:
   - Understand and know the law and the rules within your jurisdiction.
   - Understand the rules of evidence and how to ensure that the evidence is admissible in court.
   - Preplan the company's responses with law enforcement and prosecutors to understand how to handle data and conduct an investigation after a crime has been committed.
6. Information security awareness training and support:w
   - Training must be required for all workers with access to company computers and networks. Human Resources should have signed forms saying it is required and another verifying the courses taken by each employee.
   - Management must allow time for training and should encourage it.
   - Training must be customized to the contents of the policy.