The risk management task also begins in this stage. Risk management is the process of identifying, assessing, and evaluating the levels of risk facing the organization—specifically, the threats to the organization's security and to the information stored and processed by the organization. Ponder the words of the famous Chinese General Sun Tzu:

> *If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.*[10]

You begin the analysis process by getting to know your enemy. In information security, the enemy is the threats and attacks that your systems face as they provide services to your organization and its customers.

To better understand the analysis phase of the SecSDLC, you should know something about the kinds of threats facing organizations in the modern, connected world of information technology. In this context, a **threat** is a category of objects, persons, or other entities that represents a constant danger to an asset. While each enterprise's categorization of threats will almost certainly vary, threats are relatively well researched and consequently fairly well understood. To better understand the numerous threats facing an organization, a scheme has been developed to group threats by their respective activities. This model consists of 12 general categories that represent real and present dangers to an organization's information and systems. The following sections and Table 2-1, identify and describe each of these 12 categories of threats to information security.

Acts of Human Error or Failure When people use information systems, sometimes mistakes happen. Inexperience, improper training, the making of incorrect assumptions, and other

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Table 2-1 Threats to information security[11]

Source: Course Technology/Cengage Learning (adapted from Whitman, 2003)

circumstances can cause these problems. People also fail to follow policy, whether through ignorance or intent. Such failures can also threaten an organization's information assets.

Compromises to Intellectual Property The owner of intellectual property has the right to control proprietary ideas, as well as their tangible or virtual representation. Information about an organization's intellectual property can be of great interest to its competitors and can be accidentally or deliberately disseminated to those outside the organization.

Deliberate Acts of Espionage or Trespass This threat covers a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to information that an organization is trying to protect, the act is categorized as a deliberate act of espionage or trespass.

Deliberate Acts of Information Extortion Information extortion occurs when an attacker or formerly trusted insider steals information from a computer system and then demands compensation for its return or for an agreement to not disclose the information. This practice is common in credit card number theft.

Deliberate Acts of Sabotage or Vandalism This threat originates with an individual or group of individuals who intend to sabotage the operations of a computer system or business, or who perform acts of vandalism either to destroy an asset or damage the image of the organization. These threats can range from petty vandalism by employees to Web page defacement by outside persons or groups.

Deliberate Acts of Theft Theft is the illegal taking of another's property, whether physical, electronic, or intellectual.

Deliberate Software Attacks Deliberate software attacks occur when an individual or group designs software—often called malicious code or software, or malware—to attack a vulnerable system. Some of the more common types of malicious code are viruses, worms, Trojan horses, logic bombs, and back doors.

Deviations in Quality of Service by Service Providers This category includes situations in which a product or service is not delivered as expected. The organization's information system depends on the successful operation of many interdependent support systems, including power grids, telecommunications networks, parts suppliers, service vendors, and even the janitorial staff and garbage haulers.

The threat of irregularities from power utilities is common. When they occur they can lead to several types of power fluctuations:

- A voltage-level spike (a momentary increase)
- A surge (a prolonged increase)
- A momentary low voltage or sag
- A more prolonged drop in voltage, called a brownout
- A complete loss of power for a moment, called a fault
- A more lengthy loss, known as a blackout

Integrating an Organization's Mission and Objectives into the EISP

The EISP plays a number of vital roles, not the least of which is to state the importance of information security to the organization's mission and objectives. As demonstrated in the organizational and information security planning processes discussed in Chapter 2, information security strategic planning derives from the IT strategic policy, which is itself derived from the organization's strategic planning. Unless the EISP directly reflects this association, the policy will likely become confusing and counterproductive.

How can the EISP be crafted to reflect the organization's mission and objectives? Suppose that an academic institution's mission statement promotes academic freedom, independent research, and the relatively unrestricted pursuit of knowledge. This institution's EISP should reflect great tolerance for the use of organizational technology, a commitment to protecting the intellectual property of the faculty, and a degree of understanding for study delving into what could be called esoteric areas. The EISP should not contradict the organizational mission statement. For example, if the academic institution's mission statement supports the unrestricted pursuit of knowledge, then the EISP should not restrict access to pornographic Web sites or specify penalties for such access. Such a policy would directly contradict the academic institution's mission statement.

EISP Elements

Although the specifics of EISPs vary from organization to organization, most EISP documents should include the following elements:

- An overview of the corporate philosophy on security
- Information on the structure of the information security organization and individuals who fulfill the information security role
- Fully articulated responsibilities for security that are shared by all members of the organization (employees, contractors, consultants, partners, and visitors)
- Fully articulated responsibilities for security that are *unique to each role* within the organization

The components of a good EISP are shown in Table 4-1.[5]

Example EISP Components

Charles Cresson Wood, the author of *Information Security Policies Made Easy*, includes a sample high-level information security policy in his book. Table 4-2 shows some of the specific components of this model, which, when integrated into the framework described in Table 4-1, provide detailed guidance for the creation of an organization-specific EISP. In his EISP version, Wood also provides justification for each policy statement and the target audience, information that would not typically be included in the policy document itself. *Note*: Table 4-2 lists some components that could be worked into an EISP, and is not intended to represent a stand-alone EISP framework.

The formulation of the EISP establishes the overall information security environment. As noted earlier, any number of specific issues may require policy guidance beyond what can be offered in the EISP. The next level of policy document, the issue-specific policy, delivers this needed specificity.

1.	Statement of Purpose
	a. Scope and Applicability
	b. Definition of Technology Addressed
	c. Responsibilities
2.	Authorized Uses
	a. User Access
	b. Fair and Responsible Use
	c. Protection of Privacy
3.	Prohibited Uses
	a. Disruptive Use or Misuse
	b. Criminal Use
	c. Offensive or Harassing Materials
	d. Copyrighted, Licensed, or Other Intellectual Property
	e. Other Restrictions
4.	Systems Management
	a. Management of Stored Materials
	b. Employer Monitoring
	c. Virus Protection
	d. Physical Security
	e. Encryption
5.	Violations of Policy
	a. Procedures for Reporting Violations
	b. Penalties for Violations
6.	Policy Review and Modification
	a. Scheduled Review of Policy
	b. Procedures for Modification
7.	Limitations of Liability
	a. Statements of Liability
	b. Other Disclaimers

Table 4-3 Framework for issue-specific security policies

Source: Michael E. Whitman, Anthony M. Townsend, and Robert J. Alberts. Considerations for an effective telecommunications-use policy. Communications of the ACM, *June 1999, 42(6):101–109.*

defines "fair and responsible use" of equipment and other organizational assets, and it addresses key legal issues, such as protection of personal information and privacy. The policy makes any use for any purpose not explicitly identified a misuse of equipment. When it is management's intention to allow some selective, extra-organizational uses, such as using company systems and networks for noncommercial personal e-mail, that use must be allowed for in the policy.

Prohibited Uses While the previous section specifies what the issue or technology *can* be used for, this section outlines what it *cannot* be used for. Unless a particular use is clearly prohibited, the organization cannot penalize employees for it. For example, the following actions might be prohibited: personal use, disruptive use or misuse, criminal use, offensive or harassing materials, and infringement of copyrighted, licensed, or other intellectual property.

In some organizations, that which is not permitted is prohibited; while in others, that which is not prohibited is permitted. In either case, be sure to state clearly the assumptions and then spell out the exceptions. The organization's stance will make a difference in how the topic of usage is addressed. Some organizations use the approach given here that explicitly states what is allowed and prohibited. Other organizations might want to be less explicit, and might combine the Authorized and Prohibited Uses sections into a single section titled Appropriate Uses.

Systems Management This section focuses on the users' relationships to systems management. A company may want to issue specific rules regarding the use of e-mail and electronic documents, and storage of those documents, as well as guidelines about authorized employer monitoring and the physical and electronic security of e-mail and other electronic documents. The Systems Management section should specify users' and systems administrators' responsibilities, so that all parties know what they are accountable for.

Violations of Policy This section specifies the penalties and repercussions of violating the usage and systems management policies. Penalties should be laid out for each type or category of violation. This section should also provide instructions on how to report observed or suspected violations, either openly or anonymously, because some employees may fear that powerful individuals in the organization could retaliate against someone who reports violations. Anonymous submissions are often the only way to convince individual users to report the unauthorized activities of other, more influential employees.

Policy Review and Modification Every policy should contain procedures and a timetable for periodic review. This section should outline a specific methodology for the review and modification of the ISSP, so as to ensure that users always have guidelines that reflect the organization's current technologies and needs.

Limitations of Liability The final section offers a general statement of liability or a set of disclaimers. If an individual employee is caught conducting illegal activities with organizational equipment or assets, management does not want the organization to be held liable. Therefore, if employees violate a company policy or any law using company technologies, the company will not protect them and the company is not liable for their actions, assuming that the violation is not known or sanctioned by management.

Implementing the ISSP

A number of approaches for creating and managing ISSPs are possible. Three of the most common are described here:

- Create a number of independent ISSP documents, each tailored to a specific issue.
- Create a single comprehensive ISSP document that covers all issues.
- Create a modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements. This approach results in a modular document with a standard template for structure and appearance, in which

- Type of access control, whether dynamic passwords, fixed passwords, or smart cards.
- Types of user activity that will be monitored, whether files transferred, Web sites visited, or hours per day of usage.

Identification of these and other systems design decisions is ordinarily indirect. Typically a draft policy document that incorporates a number of suggested options will be prepared. Unfortunately, in an effort to expedite the policy writing process, alternative solutions are not highlighted. As a result, management may approve of a policy document incorporating decisions with far-reaching implications, many of which were unappreciated at the time of the approval. This may lead to excessive costs for information security as the initial approaches described in the policy document soon need to be replaced or revised. It may also mean that the policy document needs to be changed much sooner than it otherwise would be. […]

In organizations that have been attending to information security for some time, management will have already seriously considered all the necessary fundamental systems design options. In these cases, a policy writing effort will simply involve documenting the decisions already made, and choosing appropriate ways to express these decisions in the form of policies. In these cases, there will be no need for a separate review of the critical systems design issues as discussed above. Instead, the focus can be on the extension of these existing design decisions to new information systems such as extranets, and to new technologies such as new programming languages.

Structuring Review, Approval, and Enforcement Processes

Once the first draft of the information security policy document has been written, a few colleagues should review [it]. After the changes are made in response to feedback from these colleagues, the policy document should be sent to interested internal parties such as Internal Audit management and the Intellectual Property attorney. After a few critical allies have made changes, it is ready for review by the Information Security management committee. The next release of the draft can involve distribution to a much larger body of interested parties—for example, all information owners and all people employed in Information Systems. This review process is advisable because it builds on support from critical players, pre-selling the document to these critical players, and building support from these same critical players. […] Many review cycles, each with more changes to the policy document, are often necessary. […]

The final step in the review process is the signature of the general manager, president, chief executive officer, or chairman of the board. A brief message indicating that compliance is expected as a condition of continued employment should be found on the first page of a policy document, or the opening Web page if the policy is posted on an intranet server. This message should be signed by the top executive in a readily visible place so that the reader can have no doubt that the policy document is strongly supported by top management. […]

An information security management committee is generally composed of representatives from departments within the organization who are interested in information security. […] In most cases, Information Security management will write a draft version of

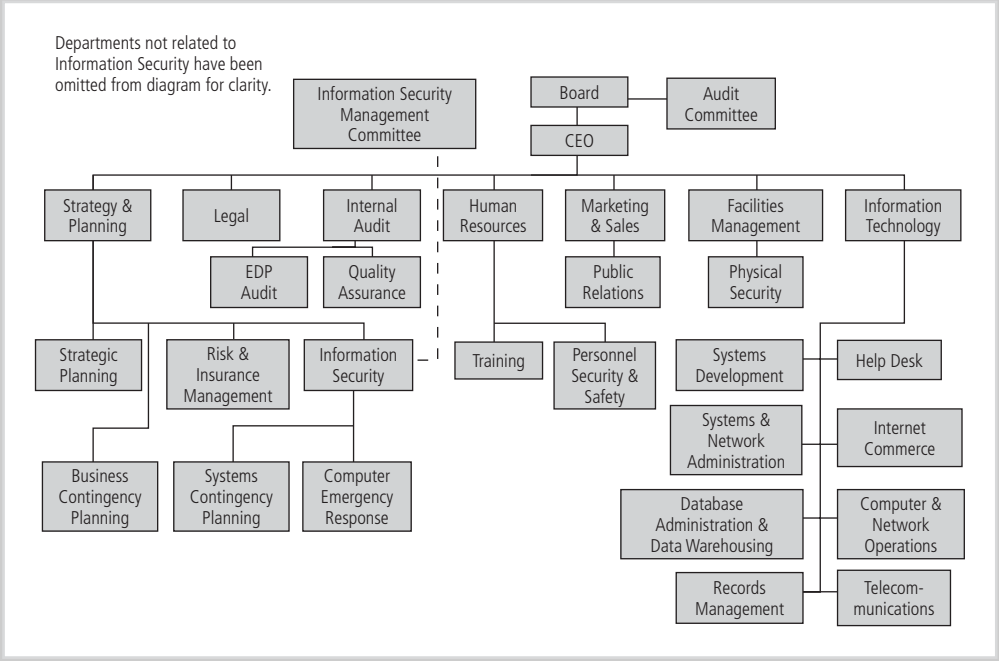

Figure 5-9 Wood's option 5: Information security reports to strategy and planning department

Source: From Information Security Roles and Responsibilities Made Easy, *used with permission.*

One problem with this approach is that the focus is strategic, and the operational and administrative aspects of information security (such as changing privileges when people change jobs) may not get the attention that they deserve from the Vice President of Strategy and Planning. On balance, though, this is an advisable reporting relationship for the information security function, and should be something that the Information Department Manager is considering for the long run even if he or she is not proposing it today.

Other Options

Other options for positioning the security department include:

- In the Legal Department: This option emphasizes copyrights, patents, trademarks, and related intellectual property protection mechanisms, as well as compliance with laws, regulations, and ethical standards (like privacy). An advantage to this reporting structure is that members of the Legal Department are comfortable with, and spend a lot of time developing, documentation such as policies and proce-dures; documentation showing that the organization is in compliance with the information security standard of due care is increasingly important.
- In the Internal Auditing Department, reporting directly to the IAD manager: Because Internal Audit is charged with reviewing the work done by other units, including the Information Security Department, this reporting structure would yield a conflict of interest.

Figure 5-15 SETA awareness components: Trinkets

Source: Course Technology/Cengage Learning

Information Security Awareness Web Site Organizations can establish Web pages or sites dedicated to promoting information security awareness, like Kennesaw State University's Web site at infosec.kennesaw.edu. As with other SETA awareness methods, the challenge lies in updating the messages frequently enough to keep them fresh. When new information is posted, employees can be informed via e-mail. The latest and archived newsletters can reside on the Web site, along with press releases, awards, and recognitions.

Here are some tips on creating and maintaining an educational Web site:[27]

1. See what's already out there. You do not have to reinvent the wheel. Look at what other organizations have done with their InfoSec awareness Web sites. Determine ownership, as you do not want to infringe on another organization's intellectual property. It is one thing to adopt a good idea; it is another thing to present it as your own. Where necessary, give credit where credit is due. A good rule of thumb is to look at a large number of sites, then design your site from memory using the best things you have seen.
2. Plan ahead. Design the Web site on paper before designing it on the computer. Standardize file naming conventions, file and image locations, and other development components, so that you do not have to recode links or pages because you changed your convention halfway through.
3. Keep page loading time to a minimum. Avoid large images and complex/long pages. Design for the lowest common denominator, typically a 640 × 480 display screen with VGA graphics. Use .jpg graphics wherever possible, as opposed to larger file formats.
4. Appearance matters. Create a themed look and feel for the pages, using templates and visually attractive formats. Keep quick links on the side, on the bottom, or in floating palettes.

Threat Identification

As mentioned at the beginning of this chapter, the ultimate goal of risk identification is to assess the circumstances and setting of each information asset to reveal any vulnerabilities. Armed with a properly classified inventory, you can assess potential weaknesses in each information asset—a process known as **threat identification**.

Any organization typically faces a wide variety of threats. If you assume that every threat can and will attack every information asset, then the project scope becomes too complex. To make the process less unwieldy, each step in the threat identification and vulnerability identification processes is managed separately and then coordinated at the end. At every step the manager is called on to exercise good judgment and draw on experience to make the process function smoothly.

Identify and Prioritize Threats and Threat Agents Chapter 2 identified 12 categories of threats to information security, which are listed alphabetically in Table 8-3.

Each of these threats presents a unique challenge to information security and must be handled with specific controls that directly address the particular threat and the threat agent's attack strategy. Before threats can be assessed in the risk identification process, however, each threat must be further examined to determine its potential to affect the targeted information asset. In general, this process is referred to as threat assessment. Posing the following questions can help you understand the threat and its potential effects on an information asset:

- *Which threats present a danger to this organization's information assets in its current environment?* Not all threats endanger every organization, of course. Examine each of the categories in Table 8-3, and eliminate any that do not apply to your organization.

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Deviations in quality of service by service provides	Power and WAN quality of service issues from service providers
Forces of nature	Fire, flood, earthquake, lightning
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Table 8-3 Threats to information security

Source: ©2003 ACM, inc., included here by permission.

Threat		Mean	Standard Deviation	Weight	Weighted Rank
1.	Deliberate software attacks	3.99	1.03	546	**2178.3**
2.	Technical software failures or errors	3.16	1.13	358	**1129.9**
3.	Acts of human error or failure	3.15	1.11	350	**1101.0**
4.	Deliberate acts of espionage or trespass	3.22	1.37	324	**1043.6**
5.	Deliberate acts of sabotage or vandalism	3.15	1.37	306	**962.6**
6.	Technical hardware failures or errors	3.00	1.18	314	**942.0**
7.	Deliberate acts of theft	3.07	1.30	226	**694.5**
8.	Forces of nature	2.80	1.09	218	**610.9**
9.	Compromises to intellectual property	2.72	1.21	182	**494.8**
10.	Quality-of-service deviations from service providers	2.65	1.06	164	**433.9**
11.	Technological obsolescence	2.71	1.11	158	**427.9**
12.	Deliberate acts of information extortion	2.45	1.42	92	**225.2**

Weighted ranks of threats to information security

Source: Adapted from M. E. Whitman. Enemy at the gates: Threats to information security. Communications of the ACM*, August 2003. Reprinted with permission.*

Another popular study also examines threats to information security. The Computer Security Institute, in cooperation with the FBI, conduct an annual survey of computer users. The following table shows its results from the last ten years.

Type of Attack or Misuse	2008	2007	2006	2005	2004	2003	2002	2001	2000	1999
Virus	50%	52%	65%	74%	78%	82%	85%	94%	85%	90%
Insider abuse of Web access	44%	59%	42%	48%	59%	80%	78%	91%	79%	97%
Laptop/mobile theft	42%	50%	47%	48%	49%	59%	55%	64%	60%	69%
Unauthorized access to information	29%	25%	32%	32%	37%	45%	38%	49%	71%	55%
Instant Messaging misuse (New category—2007)	21%	25%								
Denial of service	21%	25%	25%	32%	39%	42%	40%	36%	27%	31%
Bots within the organization (New Category—2007)	20%	21%								
Theft/loss of customer/ employee data (New category—2007)	17%	17%								

CSI/FBI survey results for types of attack or misuse (1999–2008)

Offline
Expenditures for Threats to Information Security

The *CACM* study mentioned earlier also asked computing executives to determine the priorities set in their organizations for expenditures geared toward threats to information security. Each executive responded by identifying his or her top five expenditures. These ratings were used to create a rank order of the expenses. The results are presented in the following table.

Top Threat-Driven Expenses	Rating
1. Deliberate software attacks	12.7
2. Acts of human error or failure	7.6
3. Technical software failures or errors	7.0
4. Technical hardware failures or errors	6.0
5. Quality-of-service deviations from service providers	4.9
6. Deliberate acts of espionage or trespass	4.7
7. Deliberate acts of theft	4.1
8. Deliberate acts of sabotage or vandalism	4.0
9. Technological obsolescence	3.3
10. Forces of nature	3.0
11. Compromises to intellectual property	2.2
12. Deliberate acts of information extortion	1.0

Weighted ranking of threat-driven expenditures

Source: Adapted from M. E. Whitman. Enemy at the gates: Threats to information security. Communications of the ACM*, August 2003. Reprinted with permission.*

- *Which threats would require the greatest expenditure to prevent?* Another factor that affects the danger posed by a particular threat is the amount it would cost to protect against that threat. Controlling some threats has a nominal cost, as in protections from malicious code, while other protective strategies are very expensive, as in protections from forces of nature. Here again the manager ranks, rates, or attempts to quantify the level of danger associated with protecting against a particular threat by using the same techniques outlined earlier for calculating recovery costs. Look at the Offline feature on expenditure for threats to see how some top executives recently handled this issue.

This list of questions may not cover everything that affects risk identification. An organization's specific guidelines or policies should influence the process and will inevitably require that some additional questions be answered.

Vulnerability Assessment Once you have identified the information assets of the organization and documented some threat assessment criteria, you can begin to review

every information asset for each threat. This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization. What are vulnerabilities? They are specific avenues that threat agents can exploit to attack an information asset. In other words, they are chinks in the asset's armor—a flaw or weakness in an information asset, security procedure, design, or control that can be exploited accidentally or on purpose to breach security. For example, Table 8-4 analyzes the threats to and possible vulnerabilities of a DMZ router.

A list like the one in Table 8-4 must be created for each information asset to document its vulnerability to each possible or likely attack. This list is usually long and shows all the vulnerabilities of the information asset. Some threats manifest themselves in multiple ways, yielding multiple vulnerabilities for that asset–threat pair. Of necessity, the process of listing vulnerabilities is somewhat subjective and is based on the experience and knowledge of the people who create the list. Therefore, the process works best when groups of people with diverse backgrounds work together in a series of brainstorming sessions. For instance, the team that reviews the vulnerabilities for networking equipment should include networking specialists, the systems management team that operates the network, information security risk specialists, and even technically proficient users of the system.

Threat	Possible Vulnerabilities
Acts of human error or failure	Employees or contractors may cause an outage if configuration errors are made
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of information extortion	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of sabotage or vandalism	IP is vulnerable to denial-of-service attacks Device may be subject to defacement or cache poisoning
Deliberate acts of theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate software attacks	Internet Protocol (IP) is vulnerable to denial-of-service attack; Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented
Forces of nature	All information assets in the organization are subject to forces of nature unless suitable controls are provided
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time
Technical hardware failures or errors	Hardware could fail and cause an outage Power system failures are always possible
Technical software failures or errors	Vendor-supplied routing software could fail and cause an outage
Technological obsolescence	If it is not reviewed and periodically updated, a device may fall too far behind its vendor support model to be kept in service

Table 8-4 Vulnerability assessment of a DMZ router

Source: Course Technology/Cengage Learning

more likely, however, that one or more vulnerabilities exist between the two, and as these vulnerabilities are identified, they are categorized as follows:

T1V1A1—Vulnerability 1 that exists between Threat 1 and Asset 1

T1V2A1—Vulnerability 2 that exists between Threat 1 and Asset 1

T2V1A1—Vulnerability 1 that exists between Threat 2 and Asset 1…

and so on.

In the risk assessment phase, discussed in the next section, not only are the vulnerabilities examined, but the assessment team also analyzes any existing controls that protect the asset from the threat, or mitigates the losses that may occur. Cataloging and categorizing these controls is the next step in the TVA spreadsheet.

Viewpoint
Getting at Risk

By George V. Hulme, an independent business and technology journalist who has covered information security for more than 10 years for such publications as Information Week *and* Information Security Magazine.

The risks that organizations face have never been higher. More systems are interconnected today than ever before, and there is only one constant to those systems: change. Aside from hackers, disgruntled employees, and corporate spies, a growing number of laws and regulations (such as Sarbanes-Oxley, Gramm-Leach-Bliley, and the Health Information Portability and Accountability Act) have forever changed the role of the information security professional as the gatekeeper of information and the manager of risk.

The role of the security professional is to help the organization manage risks poised against the confidentiality, integrity, and availability of its information assets. And the foundation of all information security programs begins and forever lives with the process of risk assessment. Risk isn't static. Rather, risk is fluid and evolves over time. A risk assessment conducted on the first day of the month can be quite different than the same assessment conducted several weeks later. The levels of risks for particular information systems can change as quickly as IT systems change. And geopolitical events such as war, economics, new employee hires, layoffs, and the steady introduction of new technologies all work to change the amount of risk faced by an organization.

The first task in risk assessment is to identify, assess, classify, and then decide on the value of digital assets and systems. Many believe that the most difficult aspect of risk assessment is uncovering the myriad system and configuration vulnerabilities that place systems at risk, but that's not so: An abundance of tools is available that can help automate that task. It's really deciding, organization-wide, the value of information and intellectual property that poses one of the most daunting challenges for the security professional. How much is the research and development data worth? How much will it cost the organization if it loses access to the accounting or customer relationship management systems for a day? Without knowing the value of information and the systems that ensure its flow, it's impossible to make reasonable decisions about how much can reasonably be spent protecting that information. It makes little

programmer salaries and even higher contractor expenses, the average cost to complete even a moderately sized application can quickly escalate. For example, multimedia-based training software that requires 350 hours of development for each hour of content will require the expenditure of as much as $10,000 per hour.

- Value retained from past maintenance of the information asset: It is estimated that for every dollar spent to develop an application or to acquire and process data, many more dollars are spent on maintenance over the useful life of the data or software. If actual costs have not been recorded, the cost can be estimated in terms of the human resources required to continually update, support, modify, and service the applications and systems.
- Value implied by the cost of replacing the information: The costs associated with replacing information should include the human and technical resources needed to reconstruct, restore, or regenerate the information from backups, independent transactions logs, or even hard copies of data sources. Most organizations rely on routine media backups to protect their information. When estimating recovery costs, keep in mind that you may have to hire contractors to carry out the regular workload that employees will be unable to perform during recovery efforts. Also, real-time information may not be recoverable from a tape backup, unless the system has built-in journaling capabilities. To restore this information, the various information sources may have to be reconstructed, and the data reentered into the system and validated for accuracy. This restoration can take longer than it took to create the data initially.
- Value from providing the information: Separate from the cost of developing or maintaining the information is the cost of providing the information to those users who need it. Such costs include the values associated with the delivery of the information through databases, networks, and hardware and software systems. They also include the cost of the infrastructure necessary to provide access to and control of the information.
- Value acquired from the cost of protecting the information: The value of an asset is based in part on the cost of protecting it, and the amount of money spent to protect an asset is based in part on the value of the asset. While this is a seemingly unending circle, estimating the value of protecting an information asset can help you to better understand the expense associated with its potential loss. The values listed previously are easy to calculate with some precision. This value and those that follow are likely to be estimates of cost.
- Value to owners: How much is your Social Security number worth to you? Or your telephone number? Placing a value on information can be quite a daunting task. A market researcher collects data from a company's sales figures and determines that a new product offering has a strong potential market appeal to members of a certain age group. While the cost of creating this new information may be small, how much is the new information actually worth? It could be worth millions if it successfully captures a new market share. Although it may be impossible to estimate the value of information to an organization or what portion of revenue is directly attributable to that information, it is vital to understand the overall cost that could be a consequence of its loss so as to better realize its value. Here again, estimating value may be the only method possible.
- Value of intellectual property: The value of a new product or service to a customer may ultimately be unknowable. How much would a cancer patient pay for a cure? How much would a shopper pay for a new flavor of cheese? What is the value of a logo or advertising slogan? Related but separate are intellectual properties known as trade secrets. Intellectual information assets are the primary assets of some organizations.

7. Describe the strategy of risk acceptance.
8. Describe residual risk.
9. What four types of controls or applications can be used to avoid risk?
10. Describe how outsourcing can be used for risk transference.
11. What conditions must be met to ensure that risk acceptance has been used properly?
12. What is risk appetite? Explain why risk appetite varies from organization to organization.
13. What is a cost-benefit analysis?
14. What is the difference between intrinsic value and acquired value?
15. What is single loss expectancy? What is annual loss expectancy?
16. What is the difference between benchmarking and baselining? What is the difference between due diligence and due care?
17. What is the difference between organizational feasibility and operational feasibility?
18. What is the difference between qualitative measurement and quantitative measurement?
19. What is the OCTAVE Method? What does it provide to those who adopt it?
20. How does Microsoft define risk management? What phases are used in its approach?

Exercises

1. Using the following table, calculate the SLE, ARO, and ALE for each threat category listed.

XYZ Software Company, major threat categories for new applications development (Asset value: $1,200,000 in projected revenues)		
	Cost per Incident	**Frequency of Occurrence**
Programmer Mistakes	$5,000	1 per week
Loss of Intellectual Property	$75,000	1 per year
Software Piracy	$500	1 per week
Theft of Information (Hacker)	$2,500	1 per quarter
Theft of Information (Employee)	$5,000	1 per 6 months
Web Defacement	$500	1 per month
Theft of Equipment	$5,000	1 per year
Viruses, Worms, Trojan Horses	$1,500	1 per week
Denial-of-Service Attack	$2,500	1 per quarter
Earthquake	$250,000	1 per 20 years
Flood	$250,000	1 per 10 years
Fire	$500,000	1 per 10 years

2. How did the XYZ Software Company arrive at the values in the table in Exercise 1? For each entry, describe the process of determining the cost per incident and the frequency of occurrence.
3. How do the values in the table in Exercise 1 differ from the calculations presented in the text? How can we determine SLE if there is no percentage given? Which method is easier for determining the SLE: a percentage of value lost or cost per incident?
4. Assume a year has passed and XYZ has improved its security. Using the following table, calculate the SLE, ARO, and ALE for each threat category listed.

XYZ Software Company, major threat categories for new applications development (Asset value: $1,200,000 in projected revenues)

	Cost per Incident	Frequency of Occurrence	Cost of Controls	Type of Control
Programmer Mistakes	$5,000	1 per month	$20,000	Training
Loss of Intellectual Property	$75,000	1 per 2 years	$15,000	Firewall/IDS
Software Piracy	$500	1 per month	$30,000	Firewall/IDS
Theft of Information (Hacker)	$2,500	1 per 6 months	$15,000	Firewall/IDS
Theft of Information (Employee)	$5,000	1 per year	$15,000	Physical Security
Web Defacement	$500	1 per quarter	$10,000	Firewall
Theft of Equipment	$5,000	1 per 2 year	$15,000	Physical Security
Viruses, Worms, Trojan Horses	$1,500	1 per month	$15,000	Antivirus
Denial-of-Service Attack	$2,500	1 per 6 months	$10,000	Firewall
Earthquake	$250,000	1 per 20 years	$5,000	Insurance/ Backups
Flood	$50,000	1 per 10 years	$10,000	Insurance/ Backups
Fire	$100,000	1 per 10 years	$10,000	Insurance/ Backups

Why have some values changed in the following columns: Cost per Incident and Frequency of Occurrence? How could a control affect one but not the other?

5. Assume the costs of controls presented in the table for Exercise 4 were unique costs directly associated with protecting against that threat. In other words, do not worry about overlapping costs between threats. Calculate the CBA for each control. Are they worth the costs listed?
6. Using the Web, research the costs associated with the following items when implemented by a firm with 1,000 employees and 100 servers
   - Managed antivirus software (not open source) licenses for 500 workstations

unauthorized disclosure, unauthorized use, inappropriate modification, premature deletion, and unavailability
- Regularly attends conferences, professional association meetings, and technical symposia to remain aware of the latest information security technological developments[4]

Other Position Titles Organizations often find that many (if not all) noninformation security job descriptions must define information security roles and responsibilities. The following list of positions with information security elements is drawn from *Information Security Roles and Responsibilities Made Easy* and shows the breadth of job titles that may be affected. The job description elements have been grouped according to the community of interest.

Information Security Community:

- InfoSec department manager
- Access control system administrator
- Internal InfoSec consultant
- InfoSec engineer
- InfoSec documentation specialist
- InfoSys contingency planner
- Local InfoSec coordinator

IT Community:

- Chief information officer
- InfoSys analyst/business analyst
- Systems programmer
- Business applications programmer
- Computer operations manager
- Computer operator
- InfoSys quality assurance analyst
- Help desk associate
- Archives manager/records manager
- Telecommunications manager
- Systems administrator/network administrator
- Web site administrator/commerce site administrator
- Database administrator
- Data administration manager

General Business Community:

- Physical security department manager

- Physical asset protection specialist
- Building and facilities guard
- Office maintenance worker
- Internal audit department manager
- EDP auditor
- Internal intellectual property attorney
- Human resources department manager
- Human resources consultant
- Receptionist
- Outsourcing contract administrator
- In-house trainer
- Insurance and risk management department manager
- Insurance and risk management analyst
- Business contingency planner
- Public relations manager
- Chief financial officer
- Purchasing agent
- Chief executive officer[5]

Information Security Professional Credentials

Many organizations rely to some extent on professional certifications to ascertain the level of proficiency possessed by any given candidate. Because the certification programs are relatively new, their precise value is not fully understood by most hiring organizations. The certifying bodies work diligently to educate their constituent communities on the value and qualifications of their certificate recipients. Employers struggle to match certifications to position requirements, while potential information security workers try to determine which certification programs will help them in the job market. This section identifies widely recognized information security certification programs and describes their test contents and methodologies.

(ISC)^2 Certifications

The International Information Systems Security Certification Consortium ((ISC)^2; www.isc2.org) offers security certifications, among them the Certified Information Systems Security Professional (CISSP), the Systems Security Certified Practitioner (SSCP), and the Certified Secure Software Lifecycle Professional (CSSLP).

CISSP The CISSP certification, considered to be the most prestigious certification for security managers and CISOs, recognizes mastery of an internationally identified common body of knowledge (CBK) in information security. To sit for the CISSP exam, the candidate must

Area	Act	Date	Description
Telecommunications	Telecommunications Deregulation and Competition Act of 1996—Update to Communications Act of 1934 (47 USC 151 et seq.)	1934	Regulates interstate and foreign telecommunications (amended 1996 and 2001)
Freedom of information	Freedom of Information Act (FOIA)	1966	Allows for the disclosure of previously unreleased information and documents controlled by the U.S. government
Privacy	Federal Privacy Act of 1974	1974	Governs federal agency use of personal information
Copyright	Copyright Act of 1976—Update to U.S. Copyright Law (17 USC)	1976	Protects intellectual property, including publications and software
Cryptography	Electronic Communications Privacy Act of 1986 (Update to 18 USC)	1986	Regulates interception and disclosure of electronic information; also referred to as the Federal Wiretapping Act
Access to stored communications	Unlawful Access to Stored Communications (18 USC 2701)	1986	Provides penalties for illegally accessing stored communications (such as e-mail and voicemail) stored by a service provider
Threats to computers	Computer Fraud and Abuse Act (also known as Fraud and Related Activity in Connection with Computers (18 USC 1030)	1986	Defines and formalizes laws to counter threats from computer-related acts and offenses (amended 1996, 2001, and 2006)
Federal agency information security	Computer Security Act of 1987	1987	Requires all federal computer systems that contain classified information to have security plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems
Trap and trace restrictions	General prohibition on pen register and trap and trace device use; exception (18 USC 3121 et seq.)	1993	Prohibits the use of electronic "pen registers" and trap and trace devices without a court order
Criminal intent	National Information Infrastructure Protection Act of 1996 (update to 18 USC 1030)	1996	Categorizes crimes based on defendant's authority to access a protected computer system and criminal intent
Trade Secrets	Economic Espionage Act of 1996	1996	Prevents abuse of information gained while employed elsewhere
Personal health information protection	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	1996	Requires medical practices to ensure the privacy of personal medical information

Table 12-1 **Key U.S. laws of interest to information security professionals**

this information, as well as policies and procedures to maintain them. It also requires a comprehensive assessment of the organization's information security systems, policies, and procedures. HIPAA provides guidelines for the use of electronic signatures based on security standards ensuring message integrity, user authentication, and nonrepudiation. There is no specification of particular security technologies for each of the security requirements, only that security must be implemented to ensure the privacy of the health care information.

The privacy standards of HIPAA severely restrict the dissemination and distribution of private health information without documented consent. The standards provide patients the right to know who has access to their information and who has accessed it. The privacy standards also restrict the use of health information to the minimum required for the health care services required.

HIPAA has five fundamental privacy principles:

1. Consumer control of medical information
2. Boundaries on the use of medical information
3. Accountability for the privacy of private information
4. Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
5. Security of health information

The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999 contains a number of provisions that affect banks, securities firms, and insurance companies. This act requires all financial institutions to disclose their privacy policies, describing how they share nonpublic personal information, and describing how customers can request that their information not be shared with third parties. It also ensures that the privacy policies in effect in an organization are fully disclosed when a customer initiates a business relationship and distributed at least annually for the duration of the professional association.

Export and Espionage Laws The need to protect national security, trade secrets, and a variety of other state and private assets has led to several laws affecting what information and information management and security resources may be exported from the United States (see, for example, Figure 12-1). These laws attempt to stem the theft of information by establishing strong penalties for related crimes.

To protect intellectual property and competitive advantage, Congress passed the Economic Espionage Act (EEA) in 1996. This law attempts to protect trade secrets "from the foreign government that uses its classic espionage apparatus to spy on a company, to the two American companies that are attempting to uncover each other's bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics."[11]

The Security and Freedom through Encryption Act of 1997 provides guidance on the use of encryption, and institutes measures of public protection from government intervention. Specifically, the act:

- Reinforces an individual's right to use or sell encryption algorithms, without concern for the impact of other regulations requiring some form of key registration. Key registration is when a cryptographic key (or its text equivalent) is stored with another party to be used to break the encryption of the data under some circumstances. This is often called key escrow.

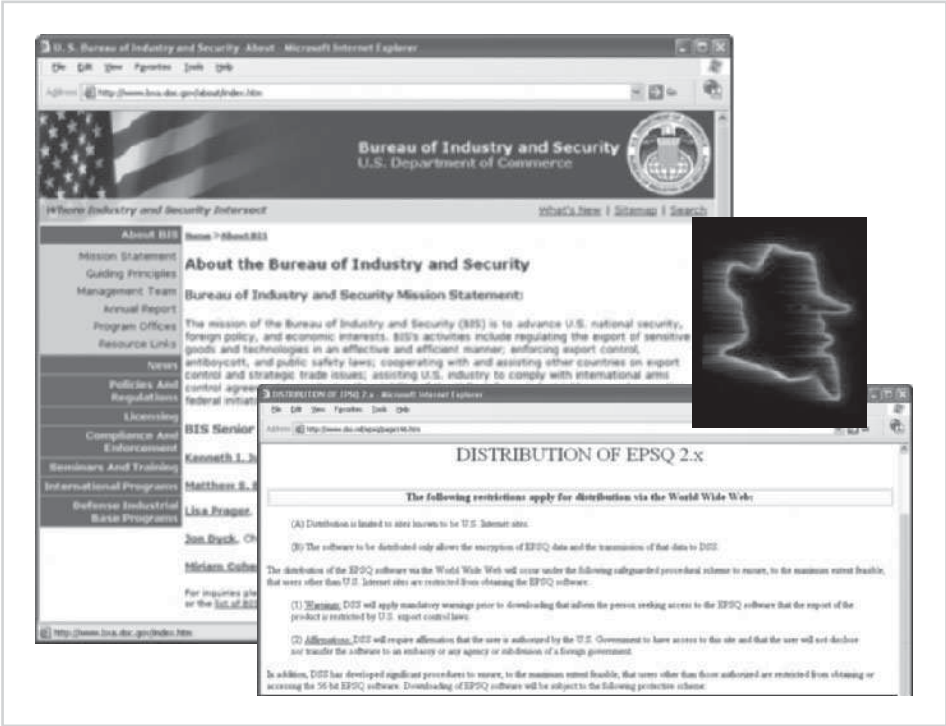

Figure 12-1 Export restrictions

Source: Course Technology/Cengage Learning

- Prohibits the federal government from requiring the use of encryption for contracts, grants, other official documents, and correspondence.
- States that the use of encryption is not probable cause to suspect criminal activity.
- Relaxes export restrictions by amending the Export Administration Act of 1979.
- Provides additional penalties for the use of encryption in the commission of a criminal act.

U.S. Copyright Law U.S. copyright law extends protection to intellectual property, which includes words published in electronic formats. The doctrine of fair use allows material to be quoted for the purpose of news reporting, teaching, scholarship, and a number of other related activities, so long as the purpose is educational and not for profit, and the usage is not excessive. Proper acknowledgement must be provided to the author and/or copyright holder of such works, including a description of the location of source materials by using a recognized form of citation.

Freedom of Information Act of 1966 (FOIA) All federal agencies are required under the Freedom of Information Act to disclose records requested in writing by any person. However, agencies may withhold information pursuant to nine exemptions and three exclusions contained in the statute. The FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local

International Laws and Legal Bodies

IT professionals and information security practitioners must realize that when their organizations do business on the Internet, they do business globally. Many domestic laws and customs do not apply to international trade, which is governed by international treaties and trade agreements. It may seem obvious, but it is often overlooked, that there are a variety of laws and ethical practices in place in other parts of the world. Different security bodies and laws are described in the following sections. Because of the political complexities of the relationships among nations and cultural differences, currently few international laws relate to privacy and information security. Therefore, these international security bodies and regulations are sometimes limited in scope and enforceability.

European Council Cyber-Crime Convention The Council of Europe drafted the European Council Cyber-Crime Convention, which empowers an international task force to oversee a range of Internet security functions and to standardize technology laws across international borders. It also attempts to improve the effectiveness of international investigations into breaches of technology law. This convention is well received by advocates of intellectual property rights, since it provides for copyright infringement prosecution.

As with any complex international legislation, the Cyber-Crime Convention lacks any realistic provisions for enforcement. The goal of the convention is to simplify the acquisition of information for law enforcement agents in certain types of international crimes, as well as the extradition process. The convention has more than its share of skeptics who see it as an attempt by the European community to exert undue influence to control a complex problem. Critics of the convention say that it could create more problems than it resolves. As the product of a number of governments, the convention tends to favor the interests of national agencies over the rights of businesses, organizations, and individuals.

Digital Millennium Copyright Act (DMCA) The Digital Millennium Copyright Act is a U.S.-based international effort to reduce the impact of copyright, trademark, and privacy infringement especially via the removal of technological copyright protection measures. The European Union also put forward Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 that increases individual rights to process and freely move personal data. The United Kingdom has already implemented a version of this directive called the Database Right.

State and Local Regulations

Each state or locality may have a number of laws and regulations that affect the use of computer technology. It is the responsibility of information security professionals to understand state laws and regulations and ensure that their organization's security policies and procedures comply with the laws and regulations.

For example, the State of Georgia passed the Georgia Computer Systems Protection Act, which has various computer security provisions and establishes specific penalties for use of information technology to attack or exploit information systems in organizations. These laws do not affect people or entities outside the state unless they do business or have offices in the state. Key provisions of this law are presented in the following details box.

It remains the individual responsibility of security professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society. It is likewise the organization's responsibility to develop, disseminate, and enforce its policies. The following sections describe several of the relevant professional associations.

Association of Computing Machinery (ACM)

The **ACM** (www.acm.org), a well-respected professional society, was originally established in 1947 as the world's first educational and scientific computing society. It is one of the few organizations that strongly promotes education and provides discounted membership for students. The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. The code contains specific references to protecting the confidentiality of information, causing no harm (with specific references to viruses), protecting the privacy of others, and respecting the intellectual property and copyrights of others. The ACM also publishes a wide variety of professional computing publications, including the highly regarded *Communications of the ACM*.

International Information Systems Security Certification Consortium, Inc. (ISC)^2

The **(ISC)^2** (www.isc2.org) is not a professional association in the strictest sense, and it has no members or membership services. It is a nonprofit organization that focuses on the development and implementation of information security certifications and credentials. The (ISC)^2 manages a body of knowledge on information security and administers and evaluates examinations for information security certifications. The code of ethics put forth by (ISC)^2 is primarily designed for information security professionals who have earned one of their certifications. This code includes four mandatory canons:

- Protect society, the commonwealth, and the infrastructure
- Act honorably, honestly, justly, responsibly, and legally
- Provide diligent and competent service to principals
- Advance and protect the profession[19]

Through this code, (ISC)^2 seeks to provide sound guidance that will enable reliance on the ethicality and trustworthiness of the information security professional as the guardian of the information and systems.

System Administration, Networking, and Security Institute (SANS)

Founded in 1989, **SANS** (www.sans.org) is a professional research and education cooperative organization. The organization, which enjoys a large professional membership, is dedicated to the protection of information and systems. Individuals who seek one of SANS's many GIAC certifications must agree to comply with the organization's code of ethics:

Respect for the Public

- I will accept responsibility in making decisions with consideration for the security and welfare of the community.

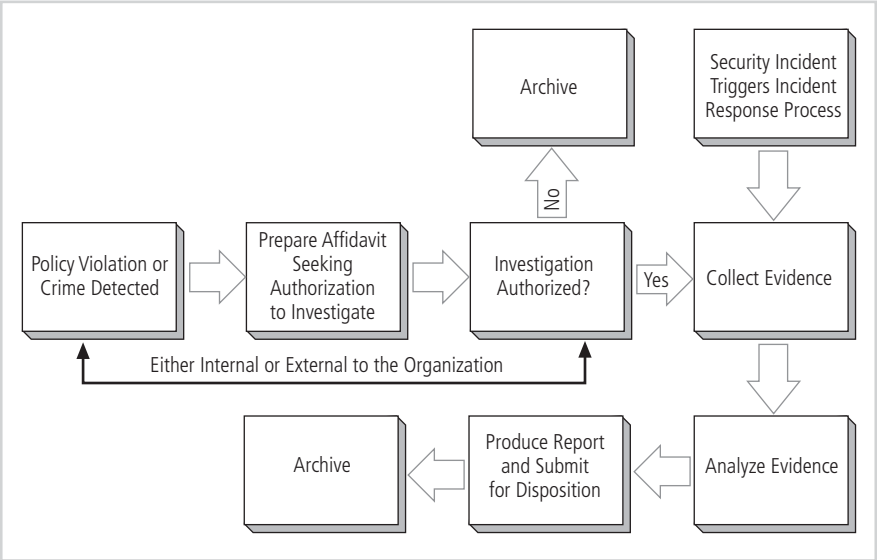

Figure 12-2 Digital forensics process

Source: Course Technology/Cengage Learning

In order to support the selection and implementation of a methodology, the organization may wish to seek legal advice or consult with local or state law enforcement. Other sources that should become part of the organization team's library are:

- Electronic Crime Scene Investigation: A Guide for First Responders (www.ncjrs.gov/pdffiles1/nij/187736.pdf)
- First Responders Guide to Computer Forensics (www.cert.org/archive/pdf/FRGCF_v1.3.pdf)
- Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (www.cybercrime.gov/s&smanual2002.htm)
- Scientific Working Group on Digital Evidence Best Practices for Computer Forensics (http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf)

Identify Relevant Items One of the crucial aspects of any digital forensic investigation is the process of identifying the potential EM and its probable location, and documenting that information in the search warrant or authorization document. Unless investigators have an idea of what to look for (such as evidence that the accused has been selling intellectual property related to future product offerings, or has been viewing objectionable or illegal content), they may never find it in the vast array of possible locations an individual user may have access to—such as flash drives, external storage drives, and Internet services.

Acquire the Evidence The principal responsibility of the response team is to acquire the information without altering it. Computers modify data constantly. Normal system file changes may be difficult to explain to a layperson (for example, a jury member with little or no technical knowledge). A normal system consequence of the search for EM could be

suitable amount of information they can summarize their findings, along with a synopsis of their investigatory procedures, in a report and submit it to the appropriate authority. This authority could be law enforcement or management. The suitable amount of EM is a flexible determination made by the investigator. In certain cases, such as child pornography, one file is sufficient to warrant turning the entire investigation over to law enforcement. On the other hand, a dismissal on the grounds of the unauthorized sale of intellectual property may require a substantial amount of information to support the organization's assertion. Reporting methods and formats vary from organization to organization and should be specified in the digital forensics policy. The general guideline for the report is that it should be sufficiently detailed to allow a similarly trained person to repeat the analysis and achieve similar results.

Evidentiary Procedures

In information security, most operations focus on policies—those documents which provide managerial guidance for ongoing implementation and operations. In digital forensics, however, the focus is on procedures. When investigating digital malfeasance or performing root cause analysis, keep in mind that the results and methods of the investigation may end up in criminal or civil court. For example, during a routine systems update, a technician finds objectionable material on an employee's computer. The employee is fired and promptly sues the organization for wrongful termination, and so the investigation of that objectionable material will come under scrutiny by the plaintiff's attorney, who will attempt to cast doubt on the ability of the investigator. While technically not illegal, the presence of the material may have been a clear violation of policy, thus prompting the dismissal of the employee, but if an attorney can convince a jury or judge that someone else could have placed the material on the plaintiff's system, then the employee could win the case and potentially a large financial settlement.

When the scenario involves criminal issues, where an employee discovers evidence of a crime, the situation changes somewhat. The investigation, analysis, and report are typically performed by law enforcement personnel. However, if the defense attorney can cast reasonable doubt on whether organizational information security professionals compromised the digital evidentiary material, the employee might win the case.

How do you avoid these legal pitfalls? Strong procedures for the handling of potential evidentiary material can minimize the probability of an organization's losing a legal challenge. Organizations should develop specific procedures, along with guidance on the use of these procedures. The policy document should specify:

- Who may conduct an investigation
- Who may authorized an investigation
- What affidavit-related documents are required
- What search warrant-related documents are required
- What digital media may be seized or taken offline
- What methodology should be followed
- What methods are required for chain of custody or chain of evidence
- What format the final report should take and to whom it should it be given

The policy document should be supported by a procedures manual, developed based on the documents discussed earlier, along with guidance from law enforcement or consultants. By creating and using these policies and procedures, an organization can best protect itself from challenges by employees who have been subject to unfavorable action (administrative or legal) resulting from an investigation.

Chapter Summary

- Laws are formally adopted rules for acceptable behavior in modern society. Ethics are socially acceptable behaviors. The key difference between laws and ethics is that laws bear the sanction of a governing authority and ethics do not.
- Organizations formalize desired behaviors in documents called policies. Unlike laws, policies must be read and explicitly agreed to by employees before they are binding.
- Civil law encompasses a wide variety of laws that regulate relationships between and among individuals and organizations. Criminal law addresses violations that harm society and that are prosecuted by the state. Tort law is a subset of civil law that deals with lawsuits by individuals rather than criminal prosecution by the state.
- The desire to protect national security, trade secrets, and a variety of other state and private assets has led to several laws affecting what information and information management and security resources may be exported from the United States.
- U.S. copyright law extends intellectual property rights to the published word, including electronic publication.
- Deterrence can prevent an illegal or unethical activity from occurring. Successful deterrence requires the institution of severe penalties, the probability of apprehension, and an expectation that penalties will be enforced.
- As part of an effort to sponsor positive ethics, a number of professional organizations have established codes of conduct or codes of ethics that their members are expected to follow.
- A number of key U.S. federal agencies charged with the protection of American information resources and the investigation of threats to, or attacks on, these resources.

Review Questions

1. What is the difference between criminal law and civil law?
2. What is tort law and what does it permit an individual to do?
3. What are the primary examples of public law?
4. Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change?
5. Which organization led the efforts to overturn the Computer Decency Act? What happened to the law it opposed?
6. What is privacy, in the context of information security?
7. What is another name for the Kennedy-Kassebaum Act (1996), and why is it important to organizations that are not in the health care industry?