chapter 8

Risk Management: Identifying and Assessing Risk

Once we know our weaknesses, they cease to do us any harm.
G. C. (Geog Christoph) Lichtenberg (1742–1799),
German Physicist and Philosopher

Iris Majwabu and Mike Edwards sat side by side on the short flight to the nearby city where the Random Widget Works, Inc. (RWW) board of directors audit committee was meeting that afternoon. The two had been invited to present RWW's information technology (IT) risk management program to the committee. The board's concerns stemmed from a recent briefing by the National Association of Corporate Directors, which focused on trends affecting the potential liability of board members in the areas of InfoSec in general and risk management in particular.

After the plane leveled off, Mike pulled out his copy of the presentation he planned to give that afternoon. He and Iris had been working on it for the past two weeks, and each knew the slides by heart. Iris was along to assist with the question-and-answer period that would follow Mike's presentation.

"They're not going to be happy campers when you're done," Iris said.

"No, they're not," Mike said. "The CEO is worried about how they'll respond and about what might come up at the full board meeting next month. I'm afraid the disconnect between IT and Internal Audit may have some unexpected consequences."

Iris considered what she knew about the weaknesses of the Internal Audit Department's approach to the company's non-IT assets. Where Mike and Iris had built a sound, fact-based

approach to estimating and controlling IT risk, some of the other company divisions used less empirical methods.

"I think we should come out of this okay," Iris told Mike. "After all, the main concern of the audit committee members is the new perception of their liability for IT security and the impact that IT risk has on the issues surrounding privacy. We have a solid risk management plan in place that's working well, in my opinion."

Mike looked up from his notes and said, "It's not us I'm worried about. I'm afraid we may create some discomfort and unwanted attention for our peers after the board sees the wide variety of risk management approaches used in other divisions."

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Define risk management and its role in the organization
- Describe risk management techniques to identify and prioritize risk factors for information assets
- Explain how risk is assessed based on the likelihood of adverse events and the effects on information assets when events occur
- Discuss the use of the results of the risk identification process

Introduction

Information security (InfoSec) in an organization exists primarily to manage IT risk. Managing risk is one of the key responsibilities of every manager within an organization. In any well-developed risk management program, two formal processes are at work. The first, risk identification and assessment, is discussed in this chapter; the second, risk control, is the subject of the next chapter.

Each manager in the organization should focus on reducing risk. This is often done within the context of one of the three communities of interest, as follows:

- General management must structure the IT and InfoSec functions in ways that will result in the successful defense of the organization's information assets, including data, hardware, software, procedures, and people.
- IT management must serve the IT needs of the broader organization and at the same time exploit the special skills and insights of the InfoSec community.
- InfoSec management must lead the way with skill, professionalism, and flexibility as it works with the other communities of interest to balance the constant trade-offs between InfoSec utility and security.

Risk Management

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.*[1]

Chinese general Sun Tzu's observation, made more than 2,400 years ago, continues to have direct relevance to the philosophy of InfoSec today. InfoSec strategy and tactics are in many ways similar to those employed in conventional warfare. InfoSec managers and technicians are the defenders of information. They constantly face a myriad of threats to the organization's information assets. A layered defense is the foundation of any InfoSec program. So, as Sun Tzu recommends, to reduce risk, an organization must (1) know itself and (2) know its enemy. This means that managers from all three communities of interest must locate the weaknesses of their organization's operations; understand how the organization's information is processed, stored, and transmitted; and identify what resources are available. Only then can they develop a strategic plan of defense.

Knowing Yourself

When operating any kind of organization, a certain amount of risk is always involved. Risk is inherent in hiring, marketing products, and even in making decisions about where to place the building that houses the organization. Risk finds its way into the daily operations of every organization, and if it is not properly managed, it can cause operational failures and even lead to complete collapse.

For an organization to manage risk properly, managers should understand how information is processed, stored, and transmitted. Knowing yourself in this context requires knowing which information assets are valuable to the organization, identifying, categorizing, and classifying those assets, and understanding how they are currently being protected. Armed with this knowledge, the organization can then initiate an in-depth risk management program. Note that the mere existence of a risk management program is not sufficient. Frequently, risk management mechanisms are implemented but not maintained or kept current. Risk management is a process, which means the safeguards and controls that are devised and implemented are not "install-and-forget" devices (see Chapter 9).

Knowing the Enemy

Once an organization becomes aware of its weaknesses, managers can take up Sun Tzu's second dictum: Know the enemy. This means identifying, examining, and understanding the threats facing the organization's information assets. Managers must be fully prepared to identify those threats that pose risks to the organization and the security of its information assets. **Risk management** is the process of discovering and assessing the risks to an organization's operations and determining how those risks can be controlled or mitigated. **Risk analysis** is the identification and assessment of levels of risk in the organization; it is a major component of risk management.

Accountability for Risk Management

All of the communities of interest bear responsibility for the management of risks. The management of the organization is accountable for the risk management program that is used. Of the three communities of interest directly linked to managing the risks to information assets, each has a particular strategic role to play:

- *InfoSec*—Because members of the InfoSec community best understand the threats and attacks that introduce risk, they often take a leadership role in addressing risk.

- *IT*—This group must help to build secure systems and ensure their safe operation. For example, IT builds and operates information systems that are mindful of operational risks and have proper controls implemented to reduce risk.
- *Management and users*—When properly trained and kept aware of the threats faced by the organization, this group plays a part in the early detection and response process. Members of this community also ensure that sufficient resources (money and personnel) are allocated to the InfoSec and IT groups to meet the security needs of the organization. For example, business managers must ensure that supporting records for orders remain intact in case of data entry error or transaction corruption. Users must be made aware of threats to data and systems and must be educated on practices that minimize those threats.

The three communities of interest must work together to address every level of risk, ranging from full-scale disasters (whether natural or human-made) to the smallest mistake made by an employee. To do so, they must be actively involved in the following activities:

- Evaluating the risk controls
- Determining which control options are cost effective
- Acquiring or installing the appropriate controls
- Overseeing processes to ensure that the controls remain effective
- Identifying risks, which includes:
  - Creating an inventory of information assets
  - Classifying and organizing those assets meaningfully
  - Assigning a value to each information asset
  - Identifying threats to the cataloged assets
  - Pinpointing vulnerable assets by tying specific threats to specific assets
- Assessing risks, which includes:
  - Determining the likelihood that vulnerable systems will be attacked by specific threats
  - Assessing the relative risk facing the organization's information assets, so that risk management and control activities can focus on assets that require the most urgent and immediate attention
  - Calculating the risks to which assets are exposed in their current setting
  - Looking in a general way at controls that might come into play for identified vulnerabilities and ways to control the risks that the assets face
  - Documenting and reporting the findings of risk identification and assessment
- Summarizing the findings, which involves stating the conclusions of the analysis stage of risk assessment in preparation for moving into the stage of controlling risk by exploring methods to mitigate risk

Figure 8-1 outlines the steps in the risk identification and assessment process.

Risk Identification

Risk identification begins with the process of self-examination. At this stage, managers *identify* the organization's information assets, *classify* and *categorize* them into useful groups, and

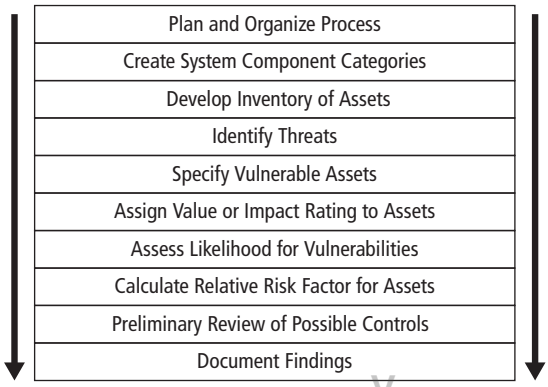

Figure 8-1 Risk identification and assessment process

prioritize them by their overall importance. This can be a daunting task, but it must be done to identify weaknesses and the threats they present.

Creating an Inventory of Information Assets

The risk identification process begins with the identification of information assets, including people, procedures, data, software, hardware, and networking elements. This step should be done

IT System Components	Risk Management Components	Example Risk Management Components
People	Internal personnel External personnel	Trusted employees Other staff members People we trust outside our organization Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Data/information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	Hardware	Systems and peripherals Security devices
Networking	Networking	Local Area Network components Intranet components Internet or extranet components Cloud-based components

Table 8-1 Organizational assets used in systems

without prejudging the value of each asset; values will be assigned later in the process. Table 8-1 shows a model outline of the identified assets subcategorized into risk management components.

The risk management components presented in Table 8-1 are organized as follows:

- The people asset is divided into internal personnel (employees) and external personnel (nonemployees). Insiders are further divided into those employees who hold trusted roles and therefore have correspondingly greater authority and accountability and those regular staff members who do not have any special privileges. Outsiders consist of other users who have access to the organization's information assets, some trusted and some untrusted.
- Procedures are assets because they are used to create value for the organization. They are divided into (1) IT and business standard procedures and (2) IT and business sensitive procedures. Sensitive procedures have the potential to enable an attack or to otherwise introduce risk to the organization. For example, the procedures used by a telecommunications company to activate new circuits pose special risks because they reveal aspects of the inner workings of a critical process, which can be subverted by outsiders for the purpose of obtaining unbilled, illicit services.
- The data asset includes information in all states: transmission, processing, and storage. This is an expanded use of the term "data," which is usually associated with databases, not the full range of information used by modern organizations.
- Software is divided into applications, operating systems, and security components. Software that provides security controls may fall into the operating systems or applications category but is differentiated by the fact that it is part of the InfoSec control environment and must therefore be protected more thoroughly than other systems components.
- Hardware is divided into (1) the usual systems devices and their peripherals and (2) the devices that are part of InfoSec control systems. The latter must be protected more thoroughly than the former.
- Networking components include networking devices (such as firewalls, routers, and switches) and the systems software within them, which is often the focal point of attacks, with successful attacks continuing against systems connected to the networks. Of course, most of today's computer systems include networking elements. You will have to determine whether a device is primarily a computer or primarily a networking device. A server computer that is used exclusively as a proxy server or bastion host may be classified as a networking component, while an identical server configured as a database server may be classified as hardware. For this reason, networking devices should be considered separately rather than combined with general hardware and software components.

In some corporate models, this list may be simplified into three groups: People, Processes and Technology, often referred to as "PPT." Whichever model is used, an organization, in the development of its risk assessment methods, should ensure that all of its information resources are properly identified, assessed, and managed for risk.

Identifying Hardware, Software, and Network Assets Many organizations use purchased asset inventory systems to keep track of their hardware, network, and perhaps their software components. Numerous packages are available in the market today, and it is up to the chief information security officer (CISO) or chief information officer (CIO) to determine which package best serves the needs of the organization. Organizations that do not use an automated inventory system must create an equivalent manual process.

Whether automated or manual, the inventory process requires a certain amount of planning. Most importantly, you must determine which attributes of each of these information assets should be tracked. That determination will depend on the needs of the organization and its risk management efforts as well as the preferences and needs of the InfoSec and IT communities. When deciding which attributes to track for each information asset, consider the following list of potential attributes:

- *Name*—This is a list of all the names commonly used for the device or program. Some organizations may have several names for the same product, and each of them should be cross-referenced in the inventory. This redundancy accommodates the usage across the organization and makes it accessible for everyone. No matter how many names you track or how you select a name, always provide a definition of the asset in question. Adopt naming standards that do not convey critical information to potential system attackers. For instance, a server named CASH1 or HQ_FINANCE may entice attackers.
- *Asset tag*—This is used to facilitate the tracking of assets. Asset tags are unique numbers assigned to assets during the acquisition process.
- *Internet Protocol (IP) address*—This attribute is useful for network devices and servers but rarely applies to software. You can, however, use a relational database and track software instances on specific servers or networking devices. Many larger organizations use the Dynamic Host Configuration Protocol (DHCP) within TCP/IP, which reassigns IP numbers to devices as needed, making the use of IP numbers as part of the asset-identification process very difficult.
- *Media Access Control (MAC) address*—As per the TCP/IP standard, all network-interface hardware devices have a unique number called the MAC address (also called an "electronic serial number" or a "hardware address"). The network operating system uses this number to identify specific network devices. The client's network software uses it to recognize traffic that it needs to process. In most settings, MAC addresses can be a useful way to track connectivity, but they can be spoofed by some hardware/software combinations. Note that some devices may have multiple network interfaces, each with its own MAC address, and others may have configurable MAC addresses, making MAC addresses even less useful as a unique identifier. Given the possibility of MAC address spoofing, the use of MAC addresses as a reliable identifier has been discontinued in many organizations.
- *Asset type*—This attribute describes the function of each asset. For hardware assets, a list of possible asset types that includes servers, desktops, networking devices, and test equipment should be developed. For software assets, a list that includes operating systems, custom applications by type (accounting, human resources, or payroll, to name a few), and packaged applications and/or specialty applications (such as firewall programs) should be developed. The degree of specificity is determined by the needs of the organization. Asset types can be recorded at two or more levels of specificity by first recording one attribute that classifies the asset at a high level and then adding attributes for more detail. For example, one server might be listed as follows:

  DeviceClass = S (server)

  DeviceOS = Win2008 (Windows 2008)

  DeviceCapacity = AS (Advanced Server)

- *Serial number*—This is a number that uniquely identifies a specific device. Some software vendors also assign a software serial number to each instance of the program licensed by the organization.
- *Manufacturer name*—This attribute can be useful for analyzing threat outbreaks when specific manufacturers announce specific vulnerabilities.
- *Manufacturer's model or part number*—This number that identifies exactly what the asset is can be very useful in the later analysis of vulnerabilities because some threats apply only to specific models of certain devices and/or software components.
- *Software version, update revision, or FCO number*—This attribute includes information about software and firmware versions and, for hardware devices, the current field change order number. A **field change order** (FCO) occurs when a manufacturer performs an upgrade to a hardware component at the customer's premises. Tracking this information is particularly important when inventorying networking devices that function mainly through the software running on them. For example, a firewall device may have three version numbers associated with it: a Basic Input/Output System (BIOS) firmware version, the running operating system version, and the firewall appliance application software version. Each organization will have to determine which of those version numbers will be tracked, or if they would like to track all three.
- *Physical location*—This attribute does not apply to software elements. Nevertheless, some organizations may have license terms that indicate where software can be used. This may include systems leased at remote locations (so-called "co-lo equipment"), often described as being "in the cloud."
- *Logical location*—This attribute specifies where an asset can be found on the organization's network. The logical location is most applicable to networking devices and indicates the logical network segment (including "virtual local area networks" or VLANs) that houses the device.
- *Controlling entity*—This refers to the organizational unit that controls the asset. In some organizations, a remote location's onsite staff could be placed in control of network devices; in other organizations, a central corporate group might control all the network devices. The inventory should determine which group controls each asset because the controlling group will want a voice in determining how much risk that device can tolerate and how much expense can be sustained to add controls.

Identifying People, Procedures, and Data Assets Human resources, documentation, and data information assets are not as readily identified and documented as hardware and software. Responsibility for identifying, describing, and evaluating these information assets should be assigned to managers who possess the necessary knowledge, experience, and judgment. As these assets are identified, they should be recorded via a reliable data-handling process like the one used for hardware and software.

The record-keeping system should be flexible, allowing you to link assets to attributes based on the nature of the information asset being tracked. Basic attributes for various classes of assets include:

People

- Position name/number/ID—Avoid names; use position titles, roles, or functions.
- Supervisor name/number/ID—Avoid names; use position titles, roles, or functions.

- Security clearance level
- Special skills

Procedures

- Description
- Intended purpose
- Software/hardware/networking elements to which the procedure is tied
- Location where procedure documents are stored for reference
- Location where it is stored for update purposes

Data

- Classification
- Owner/creator/manager
- Size of data structure
- Data structure used (e.g., sequential or relational)
- Online or offline
- Location
- Backup procedures

Consider carefully what should be tracked for specific assets. Often, larger organizations find that that they can effectively track only a few valuable facts about the most critical information assets. For instance, a company may track only IP address, server name, and device type for its mission-critical servers. The organization might forgo additional attribute tracking on all devices and completely omit the tracking of desktop or laptop systems.

Classifying and Categorizing Assets

Once the initial inventory is assembled, you must determine whether its asset categories are meaningful to the organization's risk management program. Such a review may cause managers to further subdivide the categories presented in Table 8-1 or create new categories that better meet the needs of the risk management program. For example, if the category "Internet components" is deemed too general, it could be further divided into subcategories of servers, networking devices (routers, hubs, switches), protection devices (firewalls, proxies), and cabling.

The inventory should also reflect the sensitivity and security priority assigned to each information asset. A classification scheme should be developed (or reviewed, if already in place) that categorizes these information assets based on their sensitivity and security needs. Consider the following classification scheme for an information asset: *confidential*, *internal*, and *public*. Each of these classification categories designates the level of protection needed for a particular information asset. Some asset types, such as personnel, may require an alternative classification scheme that identifies the InfoSec processes used by the asset type. For example, based on need-to-know and right-to-update, an employee might be given a certain level of security clearance, which identifies the level of information that individual is authorized to use.

Classification categories must be comprehensive and mutually exclusive. "Comprehensive" means that all inventoried assets fit into a category; "mutually exclusive" means that each asset is found in only one category. For example, an organization may have a public key

infrastructure certificate authority, which is a software application that provides cryptographic key management services. Using a purely technical standard, a manager could categorize the application in the asset list of Table 8-1 as software, a general grouping with no special classification priority. Because the certificate authority must be carefully protected as part of the InfoSec infrastructure, it should be categorized into a higher priority classification, such as *software/security component/cryptography*, and it should be verified that no overlapping category exists, such as *software/security component/PKI*.

Assessing Values for Information Assets

As each information asset is identified, categorized, and classified, a relative value must be assigned to it. Relative values are comparative judgments intended to ensure that the most valuable information assets are given the highest priority when managing risk. It may be impossible to know in advance—in absolute economic terms—what losses will be incurred if an asset is compromised; however, a relative assessment helps to ensure that the higher value assets are protected first.

As each information asset is assigned to its proper category, posing the following basic questions can help you develop the weighting criteria to be used for information asset valuation or impact evaluation. It may be useful to refer to the information collected in the business impact analysis (BIA) process (covered in Chapter 3) to help you assess a value for an asset.

- *Which information asset is the most critical to the success of the organization?* When determining the relative importance of each information asset, refer to the organization's mission statement or statement of objectives. From this source, determine which assets are essential for meeting the organization's objectives, which assets support the objectives, and which are merely adjuncts. For example, a manufacturing company that makes aircraft engines may decide that the process control systems that control the machine tools on the assembly line are the first order of importance. Although shipping and receiving data entry consoles are important to those functions, they may be less critical if alternatives are available or can be easily arranged. Another example is an online organization such as Amazon.com. The Web servers that advertise the company's products and receive its orders 24 hours a day are essential, whereas the desktop systems used by the customer service department to answer customer e-mails are less critical.
- *Which information asset generates the most revenue?* The relative value of an information asset depends on how much revenue it generates—or, in the case of a nonprofit organization, how critical it is to service delivery. Some organizations have different systems in place for each line of business or service they offer. Which of these assets plays the biggest role in generating revenue or delivering services?
- *Which information asset generates the highest profitability?* Managers should evaluate how much profit depends on a particular asset. For instance, at Amazon.com, some servers support the book sales operations, others support the auction process, and still others support the customer book review database. Which of these servers contributes the most to profitability? Although important, the review database server does not directly generate profits. Note the distinction between revenues and profits: Some systems on which revenues depend operate on thin or nonexistent margins and do not generate profits. In nonprofit organizations, you can determine what percentage of the agency's clientele receives services from the information asset being evaluated.
- *Which information asset is the most expensive to replace?* Sometimes an information asset acquires special value because it is unique. If an enterprise still uses a Model-129

keypunch machine to create special punch-card entries for a critical batch run, for example, that machine may be worth more than its cost, because spare parts or service providers may no longer be available. Another example is a specialty device with a long delivery time frame because of manufacturing or transportation requirements. Organizations must control the risk of loss or damage to such unique assets—for example, by buying and storing a backup device. Any device stored as such must, of course, be periodically updated and tested.

- *Which information asset is the most expensive to protect?* Some assets are by their nature difficult to protect, and formulating a complete answer to this question may not be possible until the risk identification phase is complete, because the costs of controls cannot be computed until the controls are identified. However, you can still make a preliminary assessment of the relative difficulty of establishing controls for each asset.
- *Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?* Almost every organization is aware of its image in the local, national, and international spheres. Loss or exposure of some assets would prove especially embarrassing. Microsoft's image, for example, was tarnished when an employee's computer system became a victim of the QAZ Trojan horse and, as a result, the latest version of Microsoft Office was stolen.[2]

You can use a worksheet, such as the one shown in Figure 8-2, to collect the answers to the preceding list of questions for later analysis.

System Name: SLS E-Commerce
Date Evaluated: February 2008
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-maill (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Figure 8-2 Sample asset classification scheme

You may also need to identify and add other institution-specific questions to the evaluation process.

Throughout this chapter, numbers are assigned to example assets to illustrate the concepts being discussed. This highlights one of the challenging issues in risk management. While other industries use actuarially derived sources to make estimates, InfoSec risk management lacks such data. Many organizations use a variety of estimating methods to assess values. Some in the industry question the use of "guesstimated" values in calculations with other estimated values, claiming this degree of uncertainty undermines the entire risk management endeavor. Research in this field is ongoing, and you are encouraged to study those sections of Chapter 9 where alternative, qualitative risk management techniques are discussed.

Listing Assets in Order of Importance

The final step in the risk identification process is to list the assets in order of importance. This goal can be achieved by using a weighted factor analysis worksheet similar to the one shown in Table 8-2. In this process, each information asset is assigned a score for each critical factor. Table 8-2 uses values from 0.1 to 1.0. Your organization may choose to use another weighting system, such as 1 to 10 or 1 to 100. Each criterion has an assigned weight showing its relative importance in the organization.

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weight (1–100); must total 100	30	40	30	
EDI Document Set 1—Logistics bill of lading to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1	1	1	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Table 8-2 Example of a weighted factor analysis worksheet

Note: EDI = Electronic Data Interchange; SSL = Secure Sockets Layer

A quick review of Table 8-2 shows that the Customer order via Secure Sockets Layer (SSL) (inbound) data flow is the most important asset on this worksheet, and that the EDI Document Set 2—Supplier fulfillment advice (inbound) is the least critical asset.

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 InfoSec, which are listed alphabetically in Table 8-3. Each of these threats presents a unique challenge to InfoSec and must be handled with specific controls that directly address the particular threat and the threat agent's attack strategy. Before

Threat	Examples
Compromises to intellectual property	Software piracy or other copyright infringement
Deviations in quality of service from service providers	Fluctuations in power, data, and other services
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, flood, earthquake, lightning, etc.
Human error or failure	Accidents, employee mistakes, failure to follow policy
Information extortion	Blackmail threat of information disclosure
Sabotage or vandalism	Damage to or destruction of systems or information
Software attacks	Malware: viruses, worms, macros, denial-of-services, or script injections
Technical hardware failures or errors	Hardware equipment failure
Technical software failures or errors	Bugs, code problems, loopholes, backdoors
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Table 8-3 Threats to InfoSec

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 various threats and their 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. It is unlikely for an organization to eliminate an entire category of threats, but doing so speeds up the threat assessment process. The Offline box titled "Threats to Information Security" describes the threats that some CIOs of major companies identified for their organizations. Although the box directly addresses only InfoSec, note that a weighted ranking of threats should be compiled for any information asset that is at risk. Once you have determined which threats apply to your organization, identify particular examples of threats within each category, eliminating those that are not relevant. For example, a company with offices on the 23rd floor of a high-rise building in Denver, Colorado, might not be subject to flooding unless they had critical infrastructure resources on a lower floor. Similarly, a firm with an office in Oklahoma City, Oklahoma, might not be concerned with landslides.
- *Which threats represent the gravest danger to the organization's information assets?* The amount of danger posed by a threat is sometimes difficult to assess. It may be tied to the probability that the threat will attack the organization, or it may reflect the amount of damage that the threat could create or the frequency with which the attack may occur. During this preliminary assessment phase, the analysis is limited to examining the existing level of preparedness and improving the strategy of InfoSec. The results should give a quick overview of the components involved.

As you will discover in Chapter 9, you can use both quantitative and qualitative measures to rank values. Since information in this case is preliminary, the organization may want to rank threats subjectively in order of danger. Alternatively, it may simply rate each of the threats on a scale of 1 to 5, with "1" designating an insignificant threat and "5" designating a highly significant threat.

Frequency of Attacks Remarkably, the number of detected attacks is steadily decreasing; after a peak in 2000, fewer organizations have reported unauthorized use of their computer systems (i.e., hacking) every year. Meanwhile, the number of organizations reporting malware attacks has dramatically increased. Unfortunately, the number of organizations willing to report the number or costs of successful attacks is also decreasing. The fact is, almost every company has experienced an attack. Whether that attack was successful depends on the company's security efforts; whether the perpetrators were caught or the organization was willing to report the attack is another matter entirely.

- *How much would it cost to recover from a successful attack?* One of the calculations that guides corporate spending on controls is the cost of recovery operations if an attack occurs and is successful. At this preliminary phase, it is not necessary to conduct a detailed assessment of the costs associated with recovering from a particular attack.

Offline
Threats to Information Security: Survey of Industry

What are the threats to InfoSec according to top computing executives?

Table 8-4 presents data collected in a study published in the Journal of Information Systems Security (JISSec) and based on a previous study published in the Communications of the ACM (CACM) that asked that very question. Based on the categories of threats presented earlier, more than 1,000 top computing executives were asked to rate each threat category on a scale ranging from "not significant" to "very significant." The results were converted to a five-point scale, where "5" represented "very significant," and are shown under the heading "Rate" in the following table. The executives were also asked to identify the top five threats to their organizations. Their responses were weighted, with five points assigned to a first-place vote and one point assigned to a fifth-place vote. The sum of weights is presented under the

2012 JISSec Ranking	Categories of Threats	Rate	Rank	Combined	2003 CACM Rank
1	Espionage or trespass	3.54	462	16.35	4
2	Software attacks	4.00	306	12.24	1
3	Human error or failure	4.30	222	9.55	3
4	Theft	3.61	162	5.85	7
5	Compromises to intellectual property	3.59	162	5.82	9
6	Sabotage or vandalism	3.11	111	3.45	5
7	Technical software failures or errors	3.17	105	3.33	2
8	Technical hardware failures or errors	2.88	87	2.51	6
9	Forces of nature	2.76	81	2.24	8
10	Deviations in quality of service from service providers	2.88	72	2.07	10
11	Technological obsolescence	2.66	57	1.52	11
12	Information extortion	2.68	18	0.48	12

Table 8-4 Weighted ranks of threats to InfoSec[3,4]

Source: Journal of Information Systems Security and Communications of the ACM.

(Continued)

heading "Rank" in the table. The two ratings were then calculated into a combined score by multiplying the two ratings and then dividing by 100. The final column shows the same threat as ranked in the 2003 CACM study.

Another popular study that examines the threats to InfoSec is the annual survey of computer users conducted by the Computer Security Institute. Table 8-5 shows biannual results since 2000.

Type of Attack or Misuse	2010/11	2008	2006	2004	2002	2000
Malware infection (revised after 2008)	67%	50%	65%	78%	85%	85%
Being fraudulently represented as sender of phishing message	39%	31%	(new category)			
Laptop/mobile hardware theft/loss	34%	42%	47%	49%	55%	60%
Bots/zombies in organization	29%	20%	(new category)			
Insider abuse of Internet access or e-mail	25%	44%	42%	59%	78%	79%
Denial-of-service	17%	21%	25%	39%	40%	27%
Unauthorized access or privilege escalation by insider	13%	15%	(revised category)			
Password sniffing	11%	9%	(new category)			
System penetration by outsider	11%		(revised category)			
Exploit of client Web browser	10%		(new category)			
Attack/Misuse categories with less than 10% responses (listed in decreasing order):						
Financial fraud						
Web site defacement						
Exploit of wireless network						
Other exploit of public-facing Web site						
Theft of or unauthorized access to PII or PHI due to all other causes						
Instant Messaging misuse						
Theft of or unauthorized access to IP due to all other causes						
Exploit of user's social network profile						
Theft of or unauthorized access to IP due to mobile device theft/loss						
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss						
Exploit of DNS server						
Extortion or blackmail associated with threat of attack or release of stolen data						

Table 8-5 CSI survey results for types of attack or misuse (2000–2011)[5]

Source: CSI surveys 2000 to 2010/11 (www.gocsi.com)

Instead, organizations often create a subjective ranking or listing of the threats based on recovery costs. Alternatively, an organization can assign a rating for each threat on a scale of 1 to 5, with "1" representing "not expensive at all" and "5" representing "extremely expensive." If the information is available, a raw value (such as $5,000, $10,000, or $2 million) can be assigned. In other words, the goal at this phase is to provide a rough assessment of the cost to recover operations should the attack interrupt normal business operations.

- *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. Some threats have a nominal cost to protect against (e.g., malicious code), while others 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. (See the Offline box on what issues executives are focusing their efforts on, financially.)

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.

Methods of Assessing Threats

A 2012 survey of computing executives also asked the following question: "In your organization's risk management efforts, what basis do you use to assess threats? (Select all that apply.)" The percentages of respondents who selected each option are shown in Table 8-6.

Vulnerability Assessment

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

Answer Options	Response Percentage
Probability of occurrence	85.4%
Reputation loss if successful	77.1%
Financial loss if successful	72.9%
Cost to protect against	64.6%
Cost to recover from successful attack	64.6%
Frequency of attack	52.1%
Competitive advantage loss if successful	35.4%
None of these	6.3%

Table 8-6 Basis of threat assessment

Offline
Expenditures for Threats to Information Security

Table 8-7 presents data from a JISSec study discussed earlier asked computing executives to list the priorities their organizations used in determining the expenditures devoted to InfoSec. Each executive responded by identifying his or her top five expenditures. A value of "5" was assigned to the highest expenditure, a value of "1" for the lowest. These ratings were used to create a rank order of the expenses. The results are presented in the following table, which compares the 2012 study with its 2003 CACM counterpart.

Threat (Based on Money and Effort Spent to Defend Against or React to It)	2012 Rating Average	2012 Ranking	2003 CACM Ranking
Espionage or trespass	4.07	1	6
Software attacks	3.94	2	1
Theft	3.18	3	7
Quality-of-service deviations by service providers	3.10	4	5
Forces of nature	3.06	5	10
Sabotage or vandalism	3.00	6	8
Technological obsolescence	2.99	7	9
Technical software failures or errors	2.71	8	3
Technical hardware failures or errors	2.64	9	4
Compromises to intellectual property	2.55	10	11
Human error or failure	2.25	11	2
Information extortion	2.00	12	12

Table 8-7 Weighted ranking of top threat-driven expenditures

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 8-8 analyzes the threats to, and possible vulnerabilities of, a DMZ router.

A list like the one in Table 8-8 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

Threat	Possible Vulnerabilities
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Forces of nature	All information assets in the organization are subject to forces of nature unless suitable controls are provided.
Human error or failure	Employees or contractors may cause an outage if configuration errors are made.
Information extortion	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time.
Sabotage or vandalism	IP is vulnerable to denial-of-service attacks. Device may be subject to defacement or cache poisoning.
Software attacks	IP is vulnerable to denial-of-service attacks. Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented.
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.
Theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.

Table 8-8 Vulnerability assessment of a DMZ router

team that reviews the vulnerabilities for networking equipment should include networking specialists, the systems management team that operates the network, InfoSec risk specialists, and even technically proficient users of the system.

The TVA Worksheet

At the end of the risk identification process, an organization should have a prioritized list of assets and their vulnerabilities. This list serves as the starting point (with its supporting documentation from the identification process) for the next step in the risk management process: risk assessment. Another list prioritizes threats facing the organization based on the weighted table discussed earlier. These two lists can be combined into a Threats-Vulnerabilities-Assets (TVA) worksheet, in preparation for the addition of vulnerability and control information during risk assessment. Along one axis lies the prioritized set of assets. Table 8-9 shows the placement of assets along the horizontal axis, with the most important asset at the left. The prioritized list of threats is placed along the vertical axis, with the most important or most dangerous threat listed at the top. The resulting grid provides a convenient method of examining the "exposure" of assets, allowing a simple

	Asset 1	Asset 2	....	....	....	....	....	....	....	....	....	Asset n
Threat 1												
Threat 2												
....												
....												
....												
....												
....												
....												
....												
....												
....												
Threat n												
Priority of Controls	1		2		3		4		5		6	
These bands of controls should be continued through all asset–threat pairs.												

Table 8-9 Sample TVA spreadsheet

vulnerability assessment. We now have a starting point for our risk assessment, along with the other documents and forms.

As you begin the risk assessment process, create a list of the TVA "triples" to facilitate your examination of the severity of the vulnerabilities. For example, between Threat 1 and Asset 1 there may or may not be a vulnerability. After all, not all threats pose risks to all assets. If a pharmaceutical company's most important asset is its research and development database and that database resides on a stand-alone network (i.e., one that is not connected to the Internet), then there may be no vulnerability to external hackers. If the intersection of T1 and A1 has no vulnerability, then the risk assessment team simply crosses out that box. It is much 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, the assessment team analyzes any existing controls that protect the asset from the threat or mitigate the losses that may occur. Cataloging and categorizing these controls is the next step in the TVA spreadsheet.

View Point
Getting at Risk

By George V. Hulme, an independent business and technology journalist who has covered information security for more than 15 years for such publications as InformationWeek 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 InfoSec 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 InfoSec 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,

(Continued)

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 are 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 sense to spend $200,000 annually to protect information that wouldn't cost an organization more than $25,000 if exposed or lost. In a perfect world, with unlimited budgets and resources in hand, everything could be protected all of the time. But we don't live in a perfect world, and tough decisions need to be made. That means bringing together management, legal, human resources, physical security, and other groups in the organization. In assessing risk, you must decide what needs to be protected and how much that information is worth. Only then can reasonable decisions be made as to how to mitigate risk by implementing defensive measures and sound policy.

During the risk assessment process, vulnerabilities to systems will inevitably be uncovered. The challenge here is to determine which ones pose the greatest threats to protected assets. It's a challenge that security professionals face every day. Does a low-risk vulnerability (something unlikely to be exploited) on a system holding highly valuable corporate information need to be remediated more quickly than a high-risk vulnerability (one that is easily and likely to be exploited) on a system holding information of little value? Maybe. It all depends. And each situation is different.

Risk can never be entirely eliminated; it can only be managed to levels that an organization can tolerate. The best way to keep risk low is to remain eternally vigilant by following a four-step process: (1) identify new assets, vulnerabilities, and threats; (2) assess and classify assets, vulnerabilities, and threats; (3) remediate and defend; and (4) return to Step 1.

Risk Assessment

Assessing the relative risk for each vulnerability is accomplished via a process called **risk assessment**. Risk assessment assigns a risk rating or score to each specific vulnerability. While this number does not mean anything in absolute terms, it enables you to gauge the relative risk associated with each vulnerable information asset, and it facilitates the creation of comparative ratings later in the risk control process.

Introduction to Risk Assessment

Estimating risk is not an exact science. Some practitioners use calculated values for risk estimation, whereas others rely on broader methods of estimation. Figure 8-3 shows the factors, some of which are estimates, that go into the risk-rating estimate for each of the vulnerabilities.

The goal is to develop a repeatable method to evaluate the *relative* risk of each of the vulnerabilities that have been identified and added to the list. Chapter 9 describes how to determine more precise costs that may be experienced from vulnerabilities that lead to losses as well as projected expenses for the controls that reduce the risks. For now, you can use the simpler risk model shown in Figure 8-3 to evaluate the risk for each information asset. The next section describes the factors used to calculate the relative risk for each vulnerability.

Likelihood

Likelihood is the overall rating—a numerical value on a defined scale—of the probability that a specific vulnerability will be exploited. In "Special Publication 800-30," NIST recommends that vulnerabilities be assigned a likelihood rating between 0.1 (low) and 1.0 (high). For example, the likelihood of an employee or system being struck by a meteorite while indoors would be rated 0.1, while the likelihood of receiving at least one e-mail containing a virus or worm in the next year would be rated 1.0. You could also choose to use a number between 1 and 100, but not 0, since vulnerabilities with a 0 likelihood should have already been removed from the asset/vulnerability list. Whatever rating system you employ for assigning likelihood, use professionalism, experience, and judgment to determine the rating—and use it consistently. Whenever possible, use external references for likelihood values, after reviewing and adjusting them for your specific circumstances. For many asset/vulnerability combinations, existing sources have already determined their likelihood. For example:

- The likelihood of a fire has been estimated actuarially for each type of structure.
- The likelihood that a given e-mail will contain a virus or worm has been researched.
- The number of network attacks can be forecast depending on how many network addresses the organization has been assigned.

Risk is

The **likelihood** of the occurrence of a vulnerability

Multiplied by

The **value** of the information asset

Minus

The percentage of risk mitigated by **current controls**

Plus

The **uncertainty** of current knowledge of the vulnerability

Figure 8-3 Risk assessment estimate factors

Assessing Potential Loss

Using the information documented during the risk identification process, you can assign weighted scores based on the value of each information asset. The actual number used will vary according to the needs of the organization. Some groups use a scale of 1–100, with "100" reserved for those information assets the loss of which would stop company operations within a few minutes. Other recommended scales, including the one in "NIST SP 800-30," use assigned weights in broad categories, with all-important assets having a value of 100, low-criticality assets having a value of 1, and all other assets having a medium value of 50. Still other scales employ weights from 1 to 10, or assigned values of 1, 3, and 5 to represent low-, medium-, and high-valued assets, respectively. Alternatively, you can create unique weighted values customized to your organization's specific needs. To be effective, the values must be assigned by asking the questions included in the section titled "Identify and Prioritize Threats and Threat Agents." These questions are restated here for easy reference:

- Which threats present a danger to this organization's assets in its current environment?
- Which threats represent the gravest danger to the organization's information assets?
- How much would it cost to recover from a successful attack?
- Which threats would require the greatest expenditure to prevent?

After reconsidering these questions, use the background information from the risk identification process and add to that information by posing yet another question:

- Which of the aforementioned questions is the most important to the protection of information from threats within this organization?

The answer to this question determines the priorities used in the assessment of vulnerabilities. Which is the most important to the organization—the cost to recover from a threat attack or the cost to protect against a threat attack? More generally, which of the threats has the highest probability of leading to a successful attack? Recall that the purpose of risk assessment is to look at the threats an organization faces in its current state. Once these questions are answered, move to the next step in the process: examining how current controls can reduce the risk faced by specific vulnerabilities.

Percentage of Risk Mitigated by Current Controls

If a vulnerability is fully managed by an existing control, it can be set aside. If it is partially controlled, estimate what percentage of the vulnerability has been controlled.

Uncertainty

It is not possible to know everything about every vulnerability, such as how likely an attack against an asset is, or how great an impact a successful attack would have on the organization. The degree to which a current control can reduce risk is also subject to estimation error. A factor that accounts for uncertainty must always be added to the equations; it consists of an estimate made by the manager using good judgment and experience.

Risk Determination

For the purpose of relative risk assessment, risk *equals* likelihood of vulnerability occurrence *times* value (or impact) *minus* percentage risk already controlled *plus* an element of uncertainty. To see how this equation works, consider the following scenario:

- Information asset A has a value score of 50 and one vulnerability: Vulnerability 1 has a likelihood of 1.0 with no current controls. You estimate that assumptions and data are 90 percent accurate.
- Information asset B has a value score of 100 and two vulnerabilities: Vulnerability 2 has a likelihood of 0.5 with a current control that addresses 50 percent of its risk; vulnerability 3 has a likelihood of 0.1 with no current controls. You estimate that assumptions and data are 80 percent accurate.

The resulting ranked list of risk ratings for the three vulnerabilities just described, using the equation *(value times likelihood) minus risk mitigated plus uncertainty*, is as follows:

- Asset A: Vulnerability 1 rated as $55 = (50 - 1.0) - 0\% + 10\%$ where
  $55 = (50 - 1.0) - ((50 - 1.0) - 0.0) + ((50 - 1.0) - 0.1)$
  $55 = 50 - 0 + 5$
- Asset B: Vulnerability 2 rated as $35 = (100 \times 0.5) - 50\% + 20\%$ where
  $35 = (100 - 0.5) - ((100 - 0.5) - 0.5) + ((100 - 0.5) - 0.2)$
  $35 = 50 - 25 + 10$
- Asset B: Vulnerability 3 rated as $12 = (100 - 0.1) - 0\% + 20\%$ where
  $12 = (100 - 0.1) - ((100 - 0.1) - 0.0) + ((100 - 0.1) - 0.2)$
  $12 = 10 - 0 + 2$

Likelihood and Consequences

Another approach to calculating risk based on likelihood is the likelihood and consequences rating from the Australian and New Zealand Risk Management Standard 4360,[6] which uses qualitative methods to determine risk based on a threat's probability of occurrence and expected results of a successful attack. **Qualitative risk assessment**, which is examined elsewhere in this chapter, consists of using categories instead of specific values to determine risk.

As shown in Table 8-10, consequences (i.e., impact assessment) are evaluated on five levels ranging from insignificant (level 1) to catastrophic (level 5). It is up to the organization to evaluate its threats and assign the appropriate consequence level.

Level	Descriptor	Example of Description
1	Insignificant	No injuries, low financial loss
2	Minor	First aid treatment, onsite release immediately contained, medium financial loss
3	Moderate	Medical treatment required, onsite release contained with outside assistance, high financial loss
4	Major	Extensive injuries, loss of production capability, offsite release with no detrimental effects, major financial loss
5	Catastrophic	Death, toxic release offsite with detrimental effect, huge financial loss

Table 8-10 Consequence levels for organizational threats[7]

Level	Descriptor	Explanation
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some time
D	Unlikely	Could occur at some time
E	Rare	May occur only in exceptional circumstances

Table 8-11 Likelihood levels for organizational threats[8]

Table 8-11 shows the qualitative likelihood assessment levels ranging from A (almost certain) to E (rare). Again, the organization must determine the likelihood or probability of an attack from each specific threat category.

When the two are combined, the organization should be able to determine which threats represent the greatest danger to the organization's information assets, as shown in Table 8-10. The resulting rankings can then be inserted into the TVA tables for use in risk assessment.

Table 8-12 identifies the potential consequences at various risk levels. If the organization has a tie in two or more threats in the same resulting category (such as Extreme Risk), then a 5A would be ranked higher than a 5B or a 4A, and so on. Replacing the A through E categories

Risk Level	Consequences				
Likelihood	Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
A (almost certain)	H	H	E	E	E
B (likely)	M	H	H	E	E
C (possible)	L	M	H	E	E
D (unlikely)	L	L	M	H	E
E (rare)	L	L	M	H	H

Table 8-12 Qualitative risk assessment matrix

Note: E = Extreme risk: Immediate action required

H = High risk: Senior management attention required

M = Moderate risk: Management responsibility must be specified

L = Low risk: Management by routine procedures required

Source: Risk management plan templates and forms from www.treasury.act.gov.au/actia/Risk.htm

with a 5 (almost certain) to 1 (rare) would allow a simple multiplication for prioritization. For example, 3 (moderate) times 4 (likely) equals 12, versus 4 (major) times 4 (likely), which equals 16.

Identify Possible Controls

For each threat and its associated vulnerabilities that have residual risk, the organization should create a preliminary list of control ideas. The purpose of this list, which begins with the identification of extant controls, is to identify areas of residual risk that may nor may not need to be reduced. **Residual risk** is the risk that remains even after the existing control has been applied. "Controls," "safeguards," and "countermeasures" are all terms used to describe security mechanisms, policies, and procedures. These mechanisms, policies, and procedures counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the general state of security within an organization.

Three general categories of controls exist: policies, programs, and technical controls. You learned about policies in Chapter 4. **Programs** are activities performed within the organization to improve security; they include security education, training, and awareness programs. Technical controls—also known as "security technologies"—are the technical implementations of the policies defined by the organization. These controls, whether in place or planned, should be added to the TVA worksheet as they are identified.

Access Controls

Access controls specifically address the admission of users into a trusted area of the organization. These areas can include information systems, physically restricted areas such as computer rooms, and even the organization in its entirety. Access controls usually consist of a combination of policies, programs, and technologies.

A number of approaches to, and categories of, access controls exist. They can be mandatory, nondiscretionary, or discretionary. Each category of controls regulates access to a particular type or collection of information, as explained in Chapter 6.

Documenting the Results of Risk Assessment

The goal of the risk management process so far has been to identify information assets and their vulnerabilities and to rank them according to the need for protection. In preparing this list, a wealth of factual information about the assets and the threats they face is collected. Also, information about the controls that are already in place is collected. The final summarized document is the ranked vulnerability risk worksheet, as shown in Table 8-9. This document is an extension of the TVA spreadsheet discussed earlier, showing only the assets and relevant vulnerabilities. A review of this worksheet reveals similarities to the weighted factor analysis worksheet depicted in Table 8-2. Table 8-13 illustrates the use of a weighted spreadsheet to calculate risk vulnerability for a number of information assets. The columns in the worksheet shown in Table 8-13 are used as follows:

- *Asset*—List each vulnerable asset.
- *Asset impact*—Show the results for this asset from the weighted factor analysis worksheet. (In our example, this value is a number from 1 to 100.)

Asset	Asset Impact	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer service request via e-mail (inbound)	55	E-mail disruption due to software failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to power failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Webserver denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.1	1
Customer order via SSL (inbound)	100	Lost orders due to Web server buffer overrun attack	0.1	1

Table 8-13 **Ranked vulnerability risk worksheet**

- *Vulnerability*—List each uncontrolled vulnerability.
- *Vulnerability likelihood*—State the likelihood of the realization of the vulnerability by a threat agent as indicated in the vulnerability analysis step. (In our example, the potential values range from 0.1 to 1.0.)
- *Risk-rating factor*—Enter the figure calculated by multiplying the asset impact and its likelihood. (In our example, the calculation yields a number ranging from 0.1 to 100.)

Looking at Table 8-13, you may be surprised that the most pressing risk requires making the mail server or servers more robust. Even though the impact rating of the information asset represented by the customer service e-mail is only 55, the relatively high likelihood of a hardware failure makes it the most pressing problem.

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns a ranked value or impact weight to each information asset
TVA worksheet	Combines the output from the information asset identification and prioritization with the threat identification and prioritization and identifies potential vulnerabilities in the "triples"; also incorporates extant and planned controls
Ranked vulnerability risk worksheet	Assigns a risk-rating ranked value to each uncontrolled asset-vulnerability pair

Table 8-14 Risk identification and assessment deliverables

Now that the risk identification process is complete, what should the documentation package look like? In other words, what are the deliverables from this stage of the risk management project? The risk identification process should designate what function the reports serve, who is responsible for preparing them, and who reviews them. The ranked vulnerability risk worksheet is the initial working document for the next step in the risk management process: assessing and controlling risk. Table 8-14 shows an example list of the worksheets that should have been prepared by an information asset risk management team up to this point.

In the last stage of the risk analysis (identification and assessment) process, you use the TVA worksheet, along with the other worksheets you have created, to develop a prioritized list of tasks. Obviously, the presence of uncontrolled vulnerabilities in high-ranking assets is the first priority for the implementation of new controls as part of the risk management process discussed in the next chapter. Before any additional controls are added, though, an organization must determine the levels of risk it is willing to accept, based on a cost-benefit analysis, which is the subject of Chapter 9.

Chapter Summary

- Risk management examines and documents an organization's information assets.
- Management is responsible for identifying and controlling the risks that an organization encounters. In the modern organization, the InfoSec group often plays a leadership role in risk management.
- A key component of a risk management strategy is the identification, classification, and prioritization of the organization's information assets.
- Assessment is the identification of assets, including all the elements of an organization's system: people, procedures, data, software, hardware, and networking elements.

- The human resources, documentation, and data information assets of an organization are not as easily identified and documented as tangible assets, such as hardware and software. These more elusive assets should be identified and described using knowledge, experience, and judgment.
- You can use the answers to the following questions to develop weighting criteria for information assets:
    - Which information asset is the most critical to the success of the organization?
    - Which information asset generates the most revenue?
    - Which information asset generates the highest profitability?
    - Which information asset is the most expensive to replace?
    - Which information asset is the most expensive to protect?
    - Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?
    - What questions should be added to cover the needs of the specific organization and its environment?
- After identifying and performing a preliminary classification of information assets, the threats facing an organization should be examined. There are 12 general categories of threats to InfoSec.
- Each threat must be examined during a threat assessment process that addresses the following questions: Which of these threats exist in this organization's environment? Which are the most dangerous to the organization's information? Which require the greatest expenditure for recovery? Which require the greatest expenditure for protection?
- Each information asset is evaluated for each threat it faces; the resulting information is used to create a list of the vulnerabilities that pose risks to the organization. This process results in an information asset and vulnerability list, which serves as the starting point for risk assessment.
- A Threats-Vulnerabilities-Assets (TVA) worksheet lists the assets in priority order along one axis, and the threats in priority order along the other axis. The resulting grid provides a convenient method of examining the "exposure" of assets, allowing a simple vulnerability assessment.
- The goal of risk assessment is the assignment of a risk rating or score that represents the relative risk for a specific vulnerability of a specific information asset.
- If any specific vulnerability is completely managed by an existing control, it no longer needs to be considered for additional controls.
- Controls, safeguards, and countermeasures should be identified for each threat and its associated vulnerabilities.
- In general, three categories of controls exist: policies, programs, and technologies.
- Access controls can be classified as mandatory, discretionary, or nondiscretionary.
- The risk identification process should designate what function the resulting reports serve, who is responsible for preparing them, and who reviews them. The TVA worksheet and the ranked vulnerability risk worksheet are the initial working documents for the next step in the risk management process: assessing and controlling risk.

Review Questions

1. What is risk management?
2. List and describe the key areas of concern for risk management.
3. Why is identification of risks, through a listing of assets and their vulnerabilities, so important to the risk management process?
4. According to Sun Tzu, what two things must be achieved to secure information assets successfully?
5. Who is responsible for risk management in an organization?
6. Which community of interest usually takes the lead in information asset risk management?
7. Which community of interest usually provides the resources used when undertaking information asset risk management?
8. In risk management strategies, why must periodic reviews be a part of the process?
9. Why do networking components need more examination from an InfoSec perspective than from a systems development perspective?
10. What value would an automated asset inventory system have for the risk identification process?
11. Which information attributes are seldom or never applied to software elements?
12. Which information attribute is often of great value for networking equipment when Dynamic Host Configuration Protocol (DHCP) is not used?
13. When you document procedures, why is it useful to know where the electronic versions are stored?
14. Which is more important to the information asset classification scheme, that it be comprehensive or that it be mutually exclusive?
15. What is the difference between an asset's ability to generate revenue and its ability to generate profit?
16. How many categories should a data classification scheme include? Why?
17. How many threat categories are listed in this chapter? Which is noted as being the most frequently encountered, and why?
18. What are vulnerabilities?
19. Describe the TVA worksheet. What is it used for?
20. Examine the simplest risk formula presented in this chapter. What are its primary elements?

Exercises

1. If an organization has three information assets to evaluate for risk management purposes, as shown in the accompanying data, which vulnerability should be evaluated for additional controls first? Which vulnerability should be evaluated last?

Data for Exercise 1:

- Switch L47 connects a network to the Internet. It has two vulnerabilities: (1) susceptibility to hardware failure, with a likelihood of 0.2, and (2) susceptibility to an SNMP buffer overflow attack, with a likelihood of 0.1. This switch has an impact rating of 90 and has no current controls in place. There is a 75 percent certainty of the assumptions and data.
- Server WebSrv6 hosts a company Web site and performs e-commerce transactions. It has Web server software that is vulnerable to attack via invalid Unicode values. The likelihood of such an attack is estimated at 0.1. The server has been assigned an impact value of 100, and a control has been implemented that reduces the impact of the vulnerability by 75 percent. There is an 80 percent certainty of the assumptions and data.
- Operators use the MGMT45 control console to monitor operations in the server room. It has no passwords and is susceptible to unlogged misuse by the operators. Estimates show the likelihood of misuse is 0.1. There are no controls in place on this asset, which has an impact rating of 5. There is a 90 percent certainty of the assumptions and data.

2. Using the Web, search for at least three tools to automate risk assessment. Collect information on automated risk assessment tools. What do they cost? What features do they provide? What are the advantages and disadvantages of each one?
3. Using the list of threats to InfoSec presented in this chapter, identify and describe three instances of each that were not mentioned in the chapter.
4. Using the data classification scheme presented in this chapter, identify and classify the information contained in your personal computer or personal digital assistant. Based on the potential for misuse or embarrassment, what information is confidential, sensitive but unclassified, or suitable for public release?
5. Using the asset valuation method presented in this chapter, conduct a preliminary risk assessment on the information contained in your home. Answer each of the valuation questions listed in the section of this chapter titled "Identify and Prioritize Threats and Threat Agents." What would it cost if you lost all your data?
6. Using the Internet, locate the National Association of Corporate Directors' Web site. Describe its function and purpose. What does this association say about board member liability for InfoSec issues?

Closing Case

Mike and Iris were flying home from the meeting. The audit committee's reaction had not been what they expected.

"I'm glad they understood the situation," Mike said. "I'd like you to start revising our risk management documentation to make it a little more general. It sounds like the board will want to take our approach company-wide soon."

Iris nodded and pulled out her notepad to make a to-do list.

Discussion

1. What will Iris have on her to-do list?
2. What resources can Iris call on to assist her?

Ethical Decision Making

Suppose that after they returned to the office, Mike was called to a private meeting with a senior executive from another division of the firm. During the discussion, Mike felt he was being subtly threatened with nonspecific but obviously devastating consequences to his career prospects at RWW as well as long-term damage to his professional reputation if he did not back off on his efforts to improve company-wide risk management at RWW. The other executive was adamant that the costs of improving the risk management process would hurt the firm without gaining any real improvement.

Was this executive simply expressing her disagreement with Mike's approach, or has some ethical line been crossed? Should Mike take any overt actions based on this conversation or inform others about the perceived threats? What could Mike do that would not embarrass the other executive and still offer him some protection in this situation?

Endnotes

1. Tzu, Sun. *The Art of War*. Translation by Samuel B. Griffith. Oxford, UK: Oxford University Press, 1988.
2. Quaglieri, Ernest. "The Hacking of Microsoft." *SANS Institute*. Accessed March 10, 2013 @ *www.giac.org/paper/gsec/488/hacking-microsoft/101184*.
3. Whitman, Michael, and Herb Mattord. "Threats to Information Security Revisited." *Journal of Information Systems Security*, 2012, 8(1).
4. Whitman, Michael. "Enemy at the Gates: Threats to Information Security." *Communications of the ACM*, August, 2003, 46(8).
5. This table is compiled from data published by the Computer Security Institute and the FBI over the years.
6. "AS/NZS 4360:1999: Risk Management." Accessed March 10, 2013 @ *www.schleupen.de/content/schleupen/schleupen013223/A.4.1.4_Australia_and_New_Zealand_Methodology_AS_NZ%25204360_1999.pdf*.
7. "Introduction to Territory Wide Risk Management: Risk Management Templates." *Australian Capital Territory Insurance Authority*. Accessed April 10, 2013 @ *www.treasury.act.gov.au/actia/RiskManagementTemplate.docx*.
8. Ibid.

Page Left Blank Intentionally

chapter 9

Risk Management: Controlling Risk

Weakness is a better teacher than strength. Weakness must learn to understand the obstacles that strength brushes aside.

MASON COOLEY, U.S. APHORIST (1927–2002)

Iris went into the manager's lounge to get a soda. As she was leaving, she saw Jane Harris—the accounting supervisor at Random Widget Works, Inc. (RWW)—at a table, poring over a spreadsheet that Iris recognized.

"Hi, Jane," Iris said. "Can I join you?"

"Sure, Iris," Jane said. "Perhaps you can help me with this form Mike wants us to fill out."

Jane was working on the asset valuation worksheet that Iris had designed to be completed by all RWW managers. The worksheet listed all of the information assets in Jane's department. Mike Edwards had asked each manager to provide three values for each item: its cost, its replacement value, and its ranked criticality to the company's mission, with the most important item being ranked number one. Mike hoped that Iris and the rest of the risk management team could use the data to build a consensus about the relative importance of various assets.

"What's the problem?" Iris asked.

"I understand these first two columns. But how am I supposed to decide what's the most important?"

"Well," Iris began, "with your accounting background, you could base your answers on some of the data you collect about each of these information assets. For this quarter, what's more important to senior management—revenue or profitability?"

"Profitability is almost always more important," Jane replied. "We have some projects that generate lots of revenue but operate at a loss."

"Well, there you go," Iris said. "Why not calculate the profitability margin for each listed item and use that to rate and rank them?"

"Oh, okay Iris. Thanks for the idea," Jane said. She then started making notes on her copy of the form.

LEARNING OBJECTIVES

Upon completion of this material, you should be able to:

- Recognize the strategy options used to control risk and be prepared to select from them when given background information
- Evaluate risk controls and formulate a cost-benefit analysis (CBA) using existing conceptual frameworks
- Explain how to maintain and perpetuate risk controls
- Describe popular approaches used in the industry to manage risk

Introduction

In the early days of information technology (IT), corporations used IT systems mainly to gain advantages over their competition. Managers discovered that establishing a competitive business model, method, or technique allowed an organization to provide a product or service that was superior in some decisive way, thus creating a competitive advantage. But this is seldom true today. The current IT industry has evolved from this earlier model to one in which almost all competitors operate using similar levels of automation. Because IT is now readily available, almost all organizations are willing to make the investment to react quickly to changes in the market. In today's highly competitive environment, managers realize that investing in IT systems at a level that merely maintains the status quo is no longer sufficient to gain a competitive advantage. In fact, even the implementation of new technologies does not necessarily enable an organization to gain or maintain a competitive lead. Instead, the concept of **competitive disadvantage**—the state of falling behind the competition—has emerged as a critical factor. Effective IT-enabled organizations now quickly absorb emerging technologies, not to gain or maintain the traditional competitive advantage but to avoid the possibility of losing market share when faltering systems make it impossible to maintain the current standard of service.

To keep up with the competition, organizations must design and create a safe environment in which business processes and procedures can function and evolve effectively. This environment must maintain confidentiality and privacy and assure the integrity and availability of organizational data. These objectives are met via the application of the principles of risk management.

This chapter builds on the concepts developed in Chapter 8, which focused on the identification of risk and the assessment of the relative impact from all identified vulnerabilities. That effort produced a list of documented vulnerabilities, ranked by criticality of impact. In this chapter, you will learn how to use such a list to assess options, estimate costs, weigh the relative merits of options, and gauge the benefits of various control approaches.

Controlling risk begins with an understanding of what risk mitigation strategies are and how to formulate them. The chosen strategy may include applying controls to some or all of the assets and vulnerabilities found in the ranked vulnerability worksheet prepared in Chapter 8. This chapter explores a variety of control approaches and then discusses how such approaches can be categorized. It also explains the critical concepts of CBA and residual risk, and it describes control strategy assessment and maintenance.

Risk Control Strategies

When an organization's general management team determines that risks from information security (InfoSec) threats are creating a competitive disadvantage, it empowers the IT and InfoSec communities of interest to control those risks. Once the project team for InfoSec development has created the ranked vulnerability worksheet (see Chapter 8), the team must choose one of five basic strategies to control the risks that arise from these vulnerabilities:

- *Defense*—Applying safeguards that eliminate or reduce the remaining uncontrolled risk
- *Transferal*—Shifting risks to other areas or to outside entities
- *Mitigation*—Reducing the impact to information assets should an attacker successfully exploit a vulnerability
- *Acceptance*—Understanding the consequences of choosing to leave a risk uncontrolled and then properly acknowledging the risk that remains without an attempt at control
- *Termination*—Removing or discontinuing the information asset from the organization's operating environment.

Defense

The **defense risk control strategy** attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities in assets, limiting access to assets, and adding protective safeguards. This approach is sometimes referred to as **avoidance**.

There are three common methods of risk defense:

- *Application of policy*—As discussed in Chapter 4, the application of policy allows all levels of management to mandate that certain procedures always be followed. For example, if the organization needs to control password use more tightly, it can implement a policy requiring passwords on all IT systems. But policy alone may not be enough. Effective management always couples changes in policy with the training and education of employees, or an application of technology, or both.
- *Application of training and education*—Communicating new or revised policy to employees may not be adequate to assure compliance. Awareness, training, and education are essential to creating a safer and more controlled organizational environment and to achieving the necessary changes in end-user behavior.
- *Implementation of technology*—In the everyday world of InfoSec, technical controls and safeguards are often required to reduce risk effectively. For example, systems administrators can configure systems to use passwords where policy requires them and where the administrators are both aware of the requirement and trained to implement it.

Risks can be avoided by countering the threats facing an asset or by eliminating the exposure of a particular asset. Eliminating the risk posed by a threat is virtually impossible, but it is possible to reduce the risk to an acceptable level.

Transferal

The **transferal risk control strategy** attempts to shift the risk to other assets, other processes, or other organizations. This goal may be accomplished by rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing insurance, or implementing service contracts with providers.

In their best-selling book *In Search of Excellence*, management consultants Thomas Peters and Robert Waterman presented case studies of high-performing corporations. One of the eight characteristics of excellent organizations is that they "stick to their knitting," the authors wrote. "They stay reasonably close to the business they know."[1] What does this mean? It means that Nabisco focuses on the manufacture and distribution of foodstuffs, while General Motors focuses on the design and manufacture of cars and trucks. Neither company spends strategic energies on the technology for securing Web sites. They focus energy and resources on what they do best while relying on consultants or contractors for other types of expertise.

Organizations should consider this whenever they begin to expand their operations, including information and systems management, and even InfoSec. When an organization does not have adequate security management and administration experience, it should hire individuals or firms that provide expertise in those areas. For example, many organizations want Web services, including Web presences, domain name registration, and domain and Web hosting. Rather than implementing their own servers and hiring their own Webmasters, Web systems administrators, and even specialized security experts, savvy organizations hire Web consulting organizations. This approach allows them to transfer the risk associated with the management of these complex systems to other organizations with more experience in dealing with those risks. A side benefit of specific contract arrangements is that the provider is responsible for disaster recovery and, through service-level agreements, for guaranteeing server and Web site availability.

Of course, outsourcing is not without its own risks. It is up to the owner of the information asset, IT management, and the InfoSec team to ensure that the disaster recovery requirements of the outsourcing contract are sufficient and have been met before they are needed.

Mitigation

The **mitigation risk control strategy** is the control approach that attempts to reduce, by means of planning and preparation, the damage caused by a realized incident or disaster. This approach includes three types of plans, which you learned about in Chapter 3: the incident response (IR) plan, the disaster recovery (DR) plan, and the business continuity (BC) plan. Mitigation depends on the ability to detect and respond to an attack as quickly as possible. As was mentioned in Chapter 3, sometimes organizations use the term "business resumption" to describe a combined DR and BC plan.

Table 9-1 summarizes the three types of mitigation plans, including descriptions and examples of each.

Acceptance

As described earlier, mitigation is a control approach that attempts to reduce the effects of an exploited vulnerability by preparing to react if and when it occurs. In contrast, the

Plan	Description	Example	When Deployed	Time frame
Incident response (IR) plan	Actions an organization takes during incidents (attacks)	• List of steps to be taken during disaster • Intelligence gathering • Information analysis	As an incident or disaster unfolds	Immediate and real-time reaction
Disaster recovery (DR) plan	• Preparations for recovery should a disaster occur • Strategies to limit losses before and during a disaster • Step-by-step instructions to regain normalcy	• Procedures for the recovery of lost data • Procedures for the reestablishment of lost services • Shutdown procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business continuity (BC) plan	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations	• Preparation steps for activation of secondary data centers • Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term organizational stability

Table 9-1 **Summary of mitigation plans**

acceptance risk control strategy is the decision to do nothing to protect an information asset from risk, and to accept the outcome from any resulting exploitation. It may or may not be a conscious business decision. Unconscious acceptance of risk is not a valid approach to risk control. Acceptance is recognized as a valid strategy *only* when the organization has:

- Determined the level of risk posed to the information asset
- Assessed the probability of attack and the likelihood of a successful exploitation of a vulnerability
- Estimated the potential damage or loss that could result from attacks
- Evaluated potential controls using each appropriate type of feasibility
- Performed a thorough CBA
- Determined that the costs to control the risk to a particular function, service, collection of data, or information asset do not justify the cost of implementing and maintaining the controls

This strategy assumes that it can be a prudent business decision to examine the alternatives and conclude that the cost of protecting an asset does not justify the security expenditure. Suppose it would cost an organization $100,000 a year to protect a server. The security assessment determines that for $10,000 the organization could replace the information contained in the server, replace the server itself, and cover all associated recovery costs. Under

those circumstances, management may be satisfied with taking its chances and saving the money that would otherwise be spent on protecting this particular asset.

An organization that decides on acceptance as a strategy for every identified risk of loss may in fact be unable to conduct proactive security activities and may have an apathetic approach to security in general. It is not acceptable for an organization to plead ignorance and thus abdicate its legal responsibility to protect employees' and customers' information. It is also unacceptable for management to hope that if they do not try to protect information, the opposition will imagine that little will be gained by an attack. The risks far outweigh the benefits of this approach, which usually ends in regret as the exploitation of the vulnerabilities causes a seemingly unending series of InfoSec lapses.

Termination

Like acceptance, the **termination risk control strategy** is based on the organization's need or choice *not* to protect an asset. Here, however, the organization does not wish the information asset to remain at risk and so removes it from the environment that represents risk.

Sometimes, the cost of protecting an asset outweighs its value. In other cases, it may be too difficult or expensive to protect an asset, compared to the value or advantage that asset offers the company. In either case, termination must be a conscious business decision, not simply the abandonment of an asset, which would technically qualify as acceptance.

Managing Risk

Risk appetite (also known as **risk tolerance**) is the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility. For instance, a financial services company, regulated by government and conservative by nature, seeks to apply every reasonable control and even some invasive controls to protect its information assets. Other less closely regulated organizations may also be conservative and thus seek to avoid the negative publicity and perceived loss of integrity caused by the exploitation of a vulnerability. A firewall vendor might install a set of firewall rules that are far more stringent than necessary, simply because being hacked would jeopardize its market. Other organizations may take on dangerous risks because of ignorance. The reasoned approach to risk is one that balances the expense (in terms of finance and the usability of information assets) against the possible losses, if exploited.

James Anderson, Executive Consultant and Director at Emagined Security, formerly a senior executive with Inovant (the world's largest commercial processor of financial payment transactions), believes that InfoSec in today's enterprise should strive to be a "well-informed sense of assurance that the information risks and controls are in balance."[2] The key is for the organization to find balance in its decision-making processes and in its feasibility analyses, thereby assuring that its risk appetite is based on experience and facts, not on ignorance or wishful thinking.

When vulnerabilities have been controlled to the degree possible, there is often remaining risk that has not been completely removed, shifted, or planned for—in other words, residual risk. **Residual risk** is the amount of risk that remains after the organization has implemented policy, education and training, and technical controls and safeguards. Figure 9-1 illustrates how residual risk persists even after safeguards are implemented, reducing the levels of risk associated with threats, vulnerabilities, and information assets.

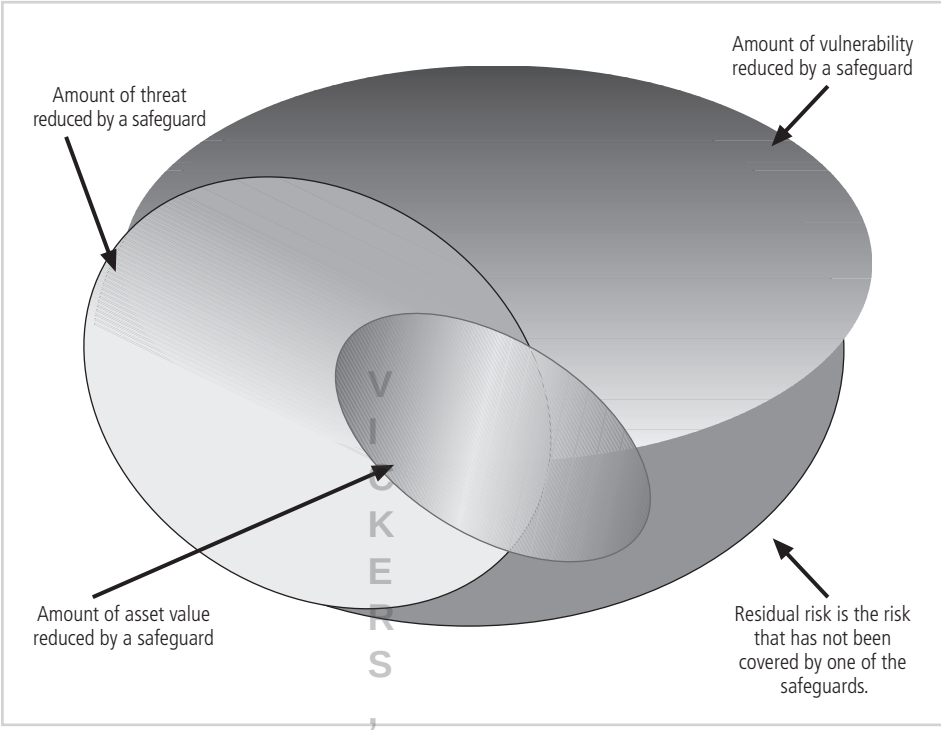

Figure 9-1 Residual risk

Although it might seem counterintuitive, the goal of InfoSec is not to bring residual risk to zero; rather, it is to bring residual risk in line with an organization's risk appetite. If decision makers have been informed of uncontrolled risks and the proper authority groups within the communities of interest decide to leave residual risk in place, then the InfoSec program has accomplished its primary goal.

Figure 9-2 illustrates the process by which an organization chooses from among the risk control strategies. As shown in this diagram, after the information system is designed, you must determine whether the system has vulnerabilities that can be exploited. If a viable threat exists, determine what an attacker will gain from a successful attack. Then, estimate the expected loss the organization will incur if the vulnerability is successfully exploited. If this loss is within the range of losses the organization can absorb, or if the attacker's gain is less than the likely cost of executing the attack, the organization may choose to accept the risk. Otherwise, it must select one of the other control strategies.

Here are some rules of thumb for selecting a strategy (keeping in mind that the level of threat and the value of the asset should play major roles in strategy selection):

- *When a vulnerability (flaw or weakness) exists in an important asset*—Implement security controls to reduce the likelihood of a vulnerability being exploited.
- *When a vulnerability can be exploited*—Apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent the occurrence of an attack.

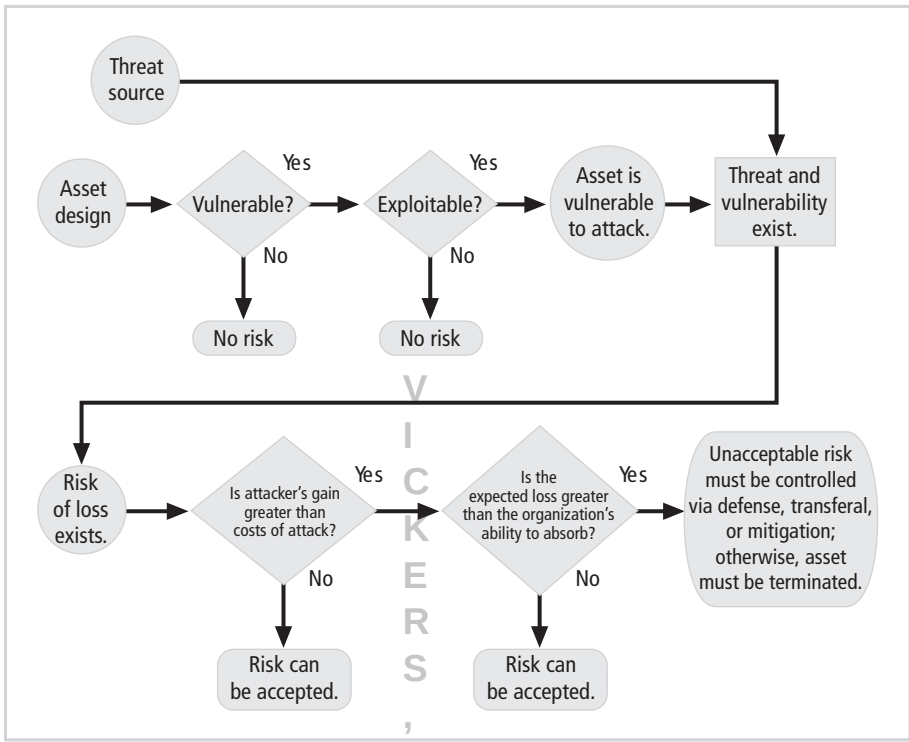

Figure 9-2 Risk-handling action points

- *When the attacker's potential gain is greater than the costs of attack*—Apply protections to increase the attacker's cost or reduce the attacker's gain by using technical or managerial controls.
- *When the potential loss is substantial*—Apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.[3]

Once a control strategy has been selected and implemented, controls should be monitored and measured on an ongoing basis to determine their effectiveness and to maintain an ongoing estimate of the remaining risk. Figure 9-3 shows how this cyclical process ensures that risks are controlled.

At a minimum, each information asset–threat pair that was developed in the risk assessment created in Chapter 8 should have a documented control strategy that clearly identifies any residual risk that remains after the proposed strategy has been executed. This approach must articulate which of the fundamental risk-reducing strategies will be used and how multiple strategies might be combined. This process must justify the selection of the chosen strategies by referencing the feasibility studies. Organizations should document the outcome of the control strategy selection process for each information asset–threat pair in an action plan. This action plan includes concrete tasks, with accountability for each task being assigned to an organizational unit or to an individual. It may include hardware and software requirements, budget estimates, and detailed timelines.

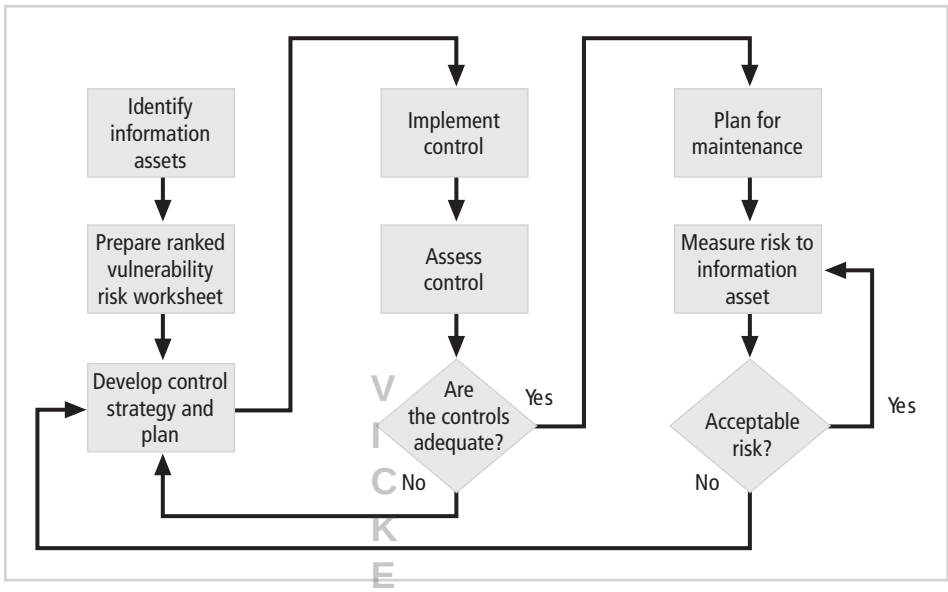

Figure 9-3 Risk control cycle

Feasibility and Cost-Benefit Analysis

Before deciding on the strategy for a specific asset–vulnerability–threat combination, an organization must explore all readily accessible information about the economic and noneconomic consequences of an exploitation of the vulnerability, when the threat causes a loss to the asset. This exploration attempts to answer the question "What are the actual and perceived advantages of implementing a control as opposed to the actual and perceived disadvantages?"

While the advantages of a specific strategy can be identified in a number of ways, the primary way is to determine the value of the information assets it is designed to protect. There are also many ways to identify the disadvantages associated with specific risk controls. The following sections describe some of the more commonly used techniques for making these choices. Some of these techniques use dollar-denominated expenses and savings from economic cost avoidance, while others use noneconomic feasibility criteria. **Cost avoidance** is the money saved by using the defense strategy via the implementation of a control, thus eliminating the financial ramifications of an incident.

Cost-Benefit Analysis

The criterion most commonly used when evaluating a strategy to implement InfoSec controls and safeguards is economic feasibility. While any number of alternatives may solve a particular problem, some are more expensive than others. Most organizations can spend only a reasonable amount of time and money on InfoSec, although the definition of "reasonable" varies from organization to organization, even from manager to manager. Organizations can begin this type of economic feasibility analysis by valuing the information assets and determining the loss in value if those information assets became compromised. Common sense

dictates that an organization should not spend more to protect an asset than it is worth. This decision-making process is called a **cost-benefit analysis** (**CBA**) or an economic feasibility study.

Cost Just as it is difficult to determine the value of information, it is difficult to determine the **cost** of safeguarding it. Among the items that affect the cost of a control or safeguard are the following:

- Cost of development or acquisition (hardware, software, and services)
- Training fees (cost to train personnel)
- Cost of implementation (installing, configuring, and testing hardware, software, and services)
- Service costs (vendor fees for maintenance and upgrades)
- Cost of maintenance (labor expense to verify and continually test, maintain, train, and update)

Benefit **Benefit** is the value to the organization of using controls to prevent losses associated with a specific vulnerability. It is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk and how much risk exists for the asset. This result is expressed as the annualized loss expectancy (ALE), which is defined later in this chapter.

Asset Valuation **Asset valuation** is the process of assigning financial value or worth to each information asset. As you learned in Chapter 8, the value of information differs within organizations and between organizations. Some argue that it is virtually impossible to accurately determine the true value of information and information-bearing assets, which is perhaps one reason why insurance underwriters currently have no definitive valuation tables for information assets. Asset valuation can draw on the assessment of information assets performed as part of the risk identification process you learned about in Chapter 8.

Asset valuation can involve the estimation of real or perceived costs. These costs can be selected from any or all of those associated with the design, development, installation, maintenance, protection, recovery, and defense against loss or litigation. Some costs are easily determined, such as the cost of replacing a network switch or the cost of the hardware needed for a specific class of server. Other costs are almost impossible to determine, such as the dollar value of the loss in market share if information on a firm's new product offerings is released prematurely and the company loses its competitive edge. A further complication is that over time some information assets acquire value that is beyond their **intrinsic value**—their essential worth. This higher **acquired value** is the more appropriate value in most cases.

Asset valuation is a complex process. While each organization must determine exactly how to value information assets, the approaches used include the following:

- *Value retained from the cost of creating the information asset*—Information is created or acquired at a cost, which can be calculated or estimated. For example, many organizations have developed extensive cost-accounting practices to capture the costs associated with collecting and processing data as well as the costs of developing and maintaining software. Software development costs include the efforts of the many

people involved in the systems development life cycle for each application and system. Although this effort draws mainly on IT personnel, it also includes the user and general management community and sometimes the InfoSec staff. In today's marketplace, with high 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, with the data reentered into the system and validated for accuracy. This restoration can take longer than it initially took to create the data.
- *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 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.
- *Value to adversaries*—How much is it worth to an organization to know what the competition is doing? Many organizations have established departments tasked with the assessment and estimation of the activities of their competition. Even organizations in traditionally nonprofit industries can benefit from knowing what is going on in political, business, and competitive organizations. Stories of industrial espionage abound, including the urban legend of Company A encouraging its employees to hire on as janitors at Company B. As custodial workers, the employees could snoop through open terminals, photograph and photocopy unsecured documents, and rifle through internal trash and recycling bins. Such legends support a widely accepted concept: Information can have extraordinary value to the right individuals. Similarly, stories are circulated of how disgruntled employees, soon to be terminated, steal information and present it to competitive organizations to curry favor and achieve new employment. Those who hire such applicants in an effort to gain from their larceny should consider whether benefiting from such a tactic is wise. After all, such thieves could presumably repeat their activities when they become disgruntled with their new employers.
- *Loss of productivity while the information assets are unavailable*—When a power failure occurs, effective use of uninterruptible power supply (UPS) equipment can prevent data loss, but users cannot create additional information. Although this is not an example of an attack that damages information, it is an instance in which a threat (deviations in quality of service from service providers) affects an organization's productivity. The hours of wasted employee time, the cost of using alternatives, and the general lack of productivity will incur costs and can severely set back a critical operation or process.
- *Loss of revenue while information assets are unavailable*—Have you ever been purchasing something at a retail store and your credit card would not scan? How many times did the salesperson rescan the card before entering the numbers manually? How long did it take to enter the numbers manually in contrast to the quick swipe? What if the credit card verification process was offline? Did the organization have a manual process to validate or process credit card payments in the absence of the familiar approval system? Many organizations have all but abandoned manual backups for automated processes. Sometimes, businesses may even have to turn away customers because their automated payments systems are inoperative. Most grocery stores no longer label each item with the price, because the UPC scanners and the related databases calculate the costs and inventory levels dynamically. Without these systems, could your grocery store sell goods? How much would the store lose if it could not? The Federal Emergency Management Agency estimates that 40 percent of businesses do not reopen after a disaster and another 25 percent fail within one year.[4] Imagine,

instead of a grocery store, an online book retailer such as Amazon.com suffering a power outage. The entire operation is instantly closed. Even if Amazon's offering system were operational, what if the payment systems were offline? Customers could make selections but could not complete their purchases. While online businesses may be more susceptible to suffering a loss of revenue as a result of a loss of information, most organizations would be unable to conduct business if certain pieces of information were unavailable.

Once an organization has estimated the worth of various assets, it can begin to calculate the potential loss from the successful exploitation of vulnerability; this calculation yields an estimate of potential loss per risk. The questions that must be asked at this stage include the following:

- What damage could occur, and what financial impact would it have?
- What would it cost to recover from the attack, in addition to the financial impact of damage?
- What is the single loss expectancy for each risk?

A **single loss expectancy** (**SLE**) is the calculated value associated with the most likely loss from a single occurrence of a specific attack. It takes into account both the value of the asset and the expected percentage of loss that would occur from a particular attack. In other words:

$$\text{SLE} = \text{asset value (AV)} \times \text{exposure factor (EF)}$$

where

EF = the percentage loss that would occur from a given vulnerability being exploited

An example would be if a Web site had an estimated value of $1,000,000 (as determined by asset valuation) and a sabotage or vandalism (hacker defacement) scenario indicated that 10 percent of the Web site would be damaged or destroyed in such an attack (the EF). In this case, the SLE for the Web site would be $1,000,000 = 0.10 \times $100,000. This estimate is then used to calculate another value, ALE, which is discussed later in this section.

As difficult as it is to estimate the value of information, estimating the probability of a threat occurrence or attack is even more difficult. There are not always tables, books, or records that indicate the frequency or probability of any given attack, although some sources are available for certain asset–threat pairs. For instance, the likelihood of a tornado or thunderstorm destroying a building of a specific type of construction within a specified region of the country is available to insurance underwriters. In most cases, however, an organization can rely only on its internal information to calculate the security of its information assets. Even if the network, systems, and security administrators have been actively and accurately tracking these threat occurrences, the organization's information will be sketchy at best. As a result, this information is usually estimated.

Usually, the probability of a threat occurring is depicted as a table that indicates how frequently an attack from each threat type is likely to occur within a given time frame (e.g., once every 10 years). This value is commonly referred to as the **annualized rate of occurrence** (ARO). ARO simply indicates how often you expect a specific type of attack to occur. For

example, if a successful act of sabotage or vandalism occurs about once every two years, then the ARO would be 50 percent (0.5). A network attack that can occur multiple times per second might be successful once each month and would have an ARO of 12.

Once you determine the loss from a single attack and the likely frequency of successful attacks, you can calculate the overall loss potential per risk expressed as an **annualized loss expectancy** (**ALE**) using the values for the ARO and SLE from the previous sections.

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

To use our previous example, if SLE = \$100,000 and ARO = 0.5, then

$$\text{ALE} = \$100{,}000 \times 0.5$$
$$\text{ALE} = \$50{,}000$$

Thus, the organization could expect to lose \$50,000 per year unless it increases its Web security. Now, armed with a figure to justify its expenditures for controls and safeguards, the InfoSec design team can deliver a budgeted value for planning purposes. Sometimes, noneconomic factors are considered in this process, so even when ALE amounts are not large, control budgets can be justified.

The CBA determines whether the benefit from a control alternative is worth the associated cost of implementing and maintaining the control. Such analyses may be performed before implementing a control or safeguard, or they can be performed after controls have been in place for a while. Observation over time adds precision to the evaluation of the benefits of the safeguard and the determination of whether the safeguard is functioning as intended. Although many CBA techniques exist, the easiest way to calculate it is by using the ALE from earlier assessments:

$$\text{CBA} = \text{ALE(precontrol)} - \text{ALE(postcontrol)} - \text{ACS}$$

where

ALE(precontrol) = ALE of the risk before the implementation of the control
ALE(postcontrol) = ALE examined after the control has been in place for a period of time
ACS = annual cost of the safeguard

Once the controls are implemented, it is crucial to examine their benefits continuously to determine when they must be upgraded, supplemented, or replaced. As Frederick Avolio states in his article "Best Practices in Network Security":

> *Security is an investment, not an expense. Investing in computer and network security measures that meet changing business requirements and risks makes it possible to satisfy changing business requirements without hurting the business's viability.*[5]

Other Methods of Establishing Feasibility

Earlier in this chapter, the concept of economic feasibility was employed to justify proposals for InfoSec controls. The next step in measuring how ready an organization is for the introduction of these controls is to determine the proposal's organizational, operational, technical, and political feasibility.

Organizational Feasibility **Organizational feasibility** analysis examines how well the proposed InfoSec alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization. In other words, the proposed control approach must contribute to the organization's strategic objectives. Does the implementation align well with the strategic planning for the information systems, or does it require deviation from the planned expansion and management of the current systems? The organization should not invest in technology that changes its fundamental ability to explore certain avenues and opportunities. For example, suppose that a university decides to implement a new firewall. It takes a few months for the technology group to learn enough about the firewall to configure it completely. A few months after the implementation begins, it is discovered that the firewall as configured does not permit outgoing Web-streamed media. If one of the goals of the university is the pursuit of distance-learning opportunities, a firewall that prevents that type of communication has not met the organizational feasibility requirement and should be modified or replaced.

Operational Feasibility **Operational feasibility** refers to user acceptance and support, management acceptance and support, and the system's compatibility with the requirements of the organization's stakeholders. Operational feasibility is also known as **behavioral feasibility**. An important aspect of systems development is obtaining user buy-in on projects. If the users do not accept a new technology, policy, or program, it will inevitably fail. Users may not openly oppose a change, but if they do not support it, they will find ways to disable or otherwise circumvent it. One of the most common methods of obtaining user acceptance and support is via user engagement. User engagement and support can be achieved by means of three simple actions: communication, education, and involvement.

Organizations should *communicate* with system users, sharing timetables and implementation schedules, plus the dates, times, and locations of upcoming briefings and training. Affected parties must know the purpose of the proposed changes and how they will enable everyone to work more securely.

In addition, users should be *educated* and trained in how to work under the new constraints while avoiding any negative performance consequences. A major frustration for users is the implementation of a new program that prevents them from accomplishing their duties, with only a promise of eventual training.

Finally, those making changes should *involve* users by asking them what they want and what they will tolerate from the new systems. One way to do so this is to include representatives from the various constituencies in the development process.

Communication, education, and involvement can reduce *resistance* to change and can build *resilience* for change—that ethereal quality that allows workers to not only tolerate constant change but also understand that change is a necessary part of the job.

Technical Feasibility Unfortunately, many organizations rush to acquire new safeguards without thoroughly examining what is required to implement and use them effectively. Because the implementation of technological controls can be extremely complex, the project team must consider their **technical feasibility**—that is, determine whether the organization already has or can acquire the technology necessary to implement and support them. For example, does the organization have the hardware and software necessary to support a new firewall system? If not, can it be obtained?

Technical feasibility analysis also examines whether the organization has the technological expertise to manage the new technology. Does the staff include individuals who are qualified (and possibly certified) to install and manage a new firewall system? If not, can staff be spared from their current obligations to attend formal training and education programs to prepare them to administer the new systems, or must personnel be hired? In the current environment, how difficult is it to find qualified personnel?

Political Feasibility Politics has been defined as "the art of the possible."[6] **Political feasibility** analysis considers what can and cannot occur based on the consensus and relationships among the communities of interest. The limits imposed by the InfoSec controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources.

In some organizations, the InfoSec community is assigned a budget, which they then allocate to activities and projects, making decisions about how to spend the money using their own judgment. In other organizations, resources are first allocated to the IT community of interest, and the InfoSec team must compete for these resources. Sometimes, the CBA and other forms of justification discussed in this chapter are used to make rational decisions about the relative merits of proposed activities and projects. Unfortunately, in other settings, these decisions are politically charged and do not focus on the pursuit of the greater organizational goals.

Another methodology for budget allocation requires the InfoSec team to propose and justify use of the resources for activities and projects in the context of the entire organization. This approach requires that arguments for InfoSec spending articulate the benefit of the expense for the whole organization, so that members of the organizational communities of interest can understand and perceive their value.

Alternatives to Feasibility Analysis

Rather than using CBA or some other feasibility reckoning to justify risk controls, an organization might look to alternative models. Many of these have been described in earlier chapters (especially in Chapter 5). A short list of alternatives is provided here:

- Benchmarking is the process of seeking out and studying the practices used in other organizations that produce the results you desire in your organization. When benchmarking, an organization typically uses either metrics-based or process-based measures.
- Due care and due diligence occur when an organization adopts a certain minimum level of security—that is, what any *prudent* organization would do in similar circumstances.
- Best business practices are considered those thought to be among the best in the industry, balancing the need to access information with adequate protection.
- The gold standard is for those ambitious organizations in which the best business practices are not sufficient. They aspire to set the standard for their industry and are thus said to be in pursuit of the gold standard.
- Government recommendations and best practices are useful for organizations that operate in industries regulated by governmental agencies. Government

View Point

The Intersection of Risk Management and Information Security

By Tim Callahan, an information technology, technology risk, and information security executive with more than 30 years' experience in the public and private sectors. Tim is currently the Senior Vice President, Business Continuity and Information Assurance, at SunTrust Bank in Atlanta, Georgia.

Many an InfoSec professional has wrestled with the topic of how risk management principles integrate with InfoSec practices. This generally rears its head when corporate is starting or refining an Enterprise Governance Risk and Compliance (EGRC) program. This article explores the complementary nature of the two programs.

For the purposes of this discussion, "information security" refers to the protection of the confidentiality, integrity, and availability of information, which includes systems, hardware, and networks that process, store, and transmit the information. As for "risk management," it involves understanding "risk" and applying the controls commensurate with the mission and goals of the organization.

At face value, we may see a paradox, or seeming contradiction, between these two concepts. One implies full protection, with less regard for cost or mission, while the other implies knowledge and judgment of the controls appropriate for the mission. A security purist might say we need to protect information at any cost, whereas someone with a risk management mindset would weigh the benefits, rewards, and practicality of controls against business objectives.

However, there is no contradiction. The InfoSec profession has matured significantly in the last decade; it has now grown beyond computer security and encompasses aspects of subdisciplines, including physical, personal, data, communications, and network security. The InfoSec professional sees these subdisciplines as interconnected, where a weakness in one affects the other. So the inclination is to ensure that all are "bolted down." This premise is correct; they are all interconnected and should be bolted down. However, over the last few years, cost and benefit discussions as well as a proliferation of security tools have influenced InfoSec practice. It is not practical to have every security tool that is available. This reality has brought about the merging of risk management practices with security practice.

As a result, one now sees job titles such as Information Risk Officer.

The majority of security professionals have embraced this concept; in fact, many would argue that the risk-based approach was always a part of the profession. There is truth to that; however, this merging has brought about a need for greater discipline in documenting risk practices. Solid risk management programs provide a formal process to understand risk, document risk, determine the organization's risk tolerance, and decide on the appropriate risk strategy.

Understanding risk begins with an "organizational" risk assessment. A good risk assessment will document the company profile: the company's purpose, its mission

(Continued)

and objectives, the risks found within the industry, the risks that are particular to the company (based on internal and external threat), and the company's tolerance for risk. As part of the assessment, risk should be considered in terms of the threat level, the regulatory environment, and the impacts to an organization's reputation. These should all be viewed from an industry-specific aspect. A bank, for instance, would have different concerns than a manufacturing company. Also, being secured in one aspect does not mean being secured in all aspects. Whereas an organization may have sound practices in addressing perceived threats, it may not be compliant with regard to its regulatory environment. Another organization may have sound practices to defend from threats and may meet all matters of regulatory compliance but still have a negative reputation with the public. All should be addressed.

Risk assessment should define controls that may be in place that reduce or mitigate the risk. The assessment should also document the strategy for risk management in terms of defense, transferal, mitigation, acceptance, or termination. Within InfoSec, there are places where the strategy should be one of termination. For instance, technology is sometimes employed that detects a threat and seeks to eliminate the threat. A simple example would be eliminating all malware. In other instances, there could be a strategy of risk acceptance if the risk is deemed low or if the protection cost far outweighs the penalty.

You may be wondering, "Why should I go to all this trouble? I just want to secure the environment!" Well, the goal of a formal risk management program is to employ a governance framework to achieve a known and consistent state—a state that can be measured, discussed, and continuously improved in an organized manner over time. Additionally, a formal program provides a way to ensure that corporate governance entities such as a corporate risk committee or the board of directors has sufficient awareness of risk and what the program is doing to address risk. One can then align the security program with the threat level, the regulatory environment, and the need to defend the organization's reputation. This will manage agreed-upon risk and help prioritize security initiatives. The program, in essence, provides a form of corporate agreement on what the security professional should be working toward. It is actually liberating in that sense.

In summary, the key to solid risk management is to understand your company's objectives, risk tolerance, and risk profile, and then make risk-based decisions that meet the company's mission and objective.

recommendations, which are, in effect, requirements, can also serve as excellent sources for information about what some organizations may be doing, or are required to do, to control InfoSec risks.

- A baseline is derived by comparing measured actual performance against established standards for the measured category.

Recommended Risk Control Practices

Assume that a risk assessment has determined it is necessary to protect a particular asset from a particular threat, at a cost of up to $50,000. Unfortunately most budget authorities focus on the "up to" and then try to cut a percentage off the total figure to save the organization money. This tendency underlines the importance of developing strong justifications for specific action plans and of providing concrete estimates in those plans.

Consider also that each control or safeguard affects more than one asset–threat pair. If a new $50,000 firewall is installed to protect the Internet connection infrastructure from hackers launching port-scanning attacks, the same firewall may also protect other information assets from other threats and attacks. The final choice may call for a balanced mixture of controls that provides the greatest value for as many asset–threat pairs as possible. This example reveals another facet of the problem: InfoSec professionals manage a dynamic matrix covering a broad range of threats, information assets, controls, and identified vulnerabilities. Each time a control is added to the matrix, it undoubtedly changes the ALE for the information asset vulnerability for which it has been designed, and it may also change the ALE for other information asset vulnerabilities. To put it more simply, if you put in one safeguard, you decrease the risk associated with all subsequent control evaluations. To make matters worse, the action of implementing a control may change the values assigned or calculated in a prior estimate.

Between the difficult task of valuing information assets and the dynamic nature of the ALE calculations, it is no wonder that organizations typically look for a more straightforward method of implementing controls. This preference has prompted an ongoing search for ways to design security architectures that go beyond the direct application of specific controls for specific information asset vulnerability. The following sections cover some of these alternatives.

Qualitative and Hybrid Measures

The steps described previously use actual values or estimates to create a quantitative assessment. In some cases, an organization might be unable to determine these values. Fortunately, risk assessment steps can be executed using estimates based on a qualitative assessment. For example, instead of placing a value of once every 10 years for the ARO, the organization might list all possible attacks on a particular set of information and rate each in terms of its probability of occurrence—high, medium, or low. The qualitative approach uses labels to assess value rather than numbers.

A more granular approach, the hybrid assessment, tries to improve upon the ambiguity of qualitative measures without resorting to the unsubstantiated estimation used for quantitative measures. Hybrid assessment uses scales rather than specific estimates. For example, a scale might range from 0, representing no chance of occurrence, to 10, representing almost certain occurrence. Organizations may, of course, prefer other scales: 0–10, 1–5, 0–20. These same scales can be used in any situation requiring a value, even in asset valuation. For example, instead of estimating that a particular piece of information is worth $1,000,000, you might value information on a scale of 1–20, where 1 indicates relatively worthless information and 20 indicates extremely critical information, such as

a certain soda manufacturer's secret recipe or the 11 herbs and spices of a popular chicken vendor.

Delphi Technique

How do you calculate the values and scales used in qualitative and quantitative assessment? An individual can pull the information together based on personal experience, but, as the saying goes, "two heads are better than one"—and a team of heads is better than two. The **Delphi technique**, named for the oracle at Delphi, which predicted the future (in Greek mythology), is a process whereby a group rates or ranks a set of information. The individual responses are compiled and then returned to the group for another iteration. This process continues until the entire group is satisfied with the result. This technique can be applied to the development of scales, asset valuation, asset or threat ranking, or any scenario that can benefit from the input of more than one decision maker.

The OCTAVE Methods

Until now, this book has presented a general treatment of risk management, synthesizing information and methods from many sources to present the customary or usual approaches that organizations use to manage risk. This and the following sections present alternative approaches to risk management that come from a single source. One such source, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method, is an InfoSec risk evaluation methodology that allows organizations to balance the protection of critical information assets against the costs of providing protective and detection controls. This process can enable an organization to measure itself against known or accepted good security practices and then establish an organization-wide protection strategy and InfoSec risk mitigation plan. (For more detailed information about the OCTAVE Method, you can download its implementation guide from *www.cert.org/octave/omig.html*.)

Promoted by the Computer Emergency Response Team (CERT) Coordination Center (*www.cert.org*), the OCTAVE process can enable an organization to measure itself against known and accepted good security practices and then establish an organization-wide protection strategy and InfoSec risk mitigation plan. There are three variations of the OCTAVE Method:

- The original OCTAVE Method, which forms the basis for the OCTAVE body of knowledge and which was designed for large organizations (300 or more users)
- OCTAVE-S, for smaller organizations of about 100 users
- OCTAVE-Allegro, a streamlined approach for InfoSec assessment and assurance

For more information on these OCTAVE methods, see *www.cert.org/octave*.

Microsoft Risk Management Approach

Microsoft has recently updated its Security Risk Management Guide, which can be found at *http://technet.microsoft.com/en-us/library/cc163143.aspx*. The guide provides the company's approach to the risk management process. Because this version is comprehensive, easily

scalable, and repeatable, it is summarized here and discussed in additional detail in the Appendix.[7]

Microsoft asserts that risk management is not a stand-alone subject and should be part of a general governance program to allow the organizational general-management community of interest to evaluate the organization's operations and make better, more informed decisions. The purpose of the risk management process is to prioritize and manage security risks. Microsoft presents four phases in its security risk management process:

1. Assessing risk
2. Conducting decision support
3. Implementing controls
4. Measuring program effectiveness

These four phases, which are described in detail in the Appendix, provide an overview of a program that is similar to the methods presented earlier in the text, including the OCTAVE Method. Microsoft, however, breaks the phases into fewer, more manageable pieces.

FAIR

Factor Analysis of Information Risk (FAIR), a risk management framework developed by Jack A. Jones, can help organizations understand, analyze, and measure information risk. The outcomes are more cost-effective information risk management, greater credibility for the InfoSec profession, and a foundation from which to develop a scientific approach to information risk management. The FAIR framework, as described on the host Web site (*http://fairwiki.riskmanagementinsight.com*), includes:

- A taxonomy for information risk
- Standard nomenclature for information risk terms
- A framework for establishing data collection criteria
- Measurement scales for risk factors
- A computational engine for calculating risk
- A modeling construct for analyzing complex risk scenarios

Basic FAIR analysis comprises 10 steps in four stages:

Stage 1—Identify Scenario Components

1. Identify the asset at risk.
2. Identify the threat community under consideration.

Stage 2—Evaluate Loss Event Frequency (LEF)

3. Estimate the probable Threat Event Frequency (TEF).
4. Estimate the Threat Capability (TCap).
5. Estimate Control Strength (CS).

6. Derive Vulnerability (Vuln).
7. Derive Loss Event Frequency (LEF).

Stage 3—Evaluate Probable Loss Magnitude (PLM)

8. Estimate worst-case loss.
9. Estimate probable loss.

Stage 4—Derive and Articulate Risk

10. Derive and articulate risk.

Unlike other risk management frameworks, FAIR relies on the qualitative assessment of many risk components, using scales with value ranges—for example, very high to very low. Figure 9-4 shows the basic structure of the FAIR method.

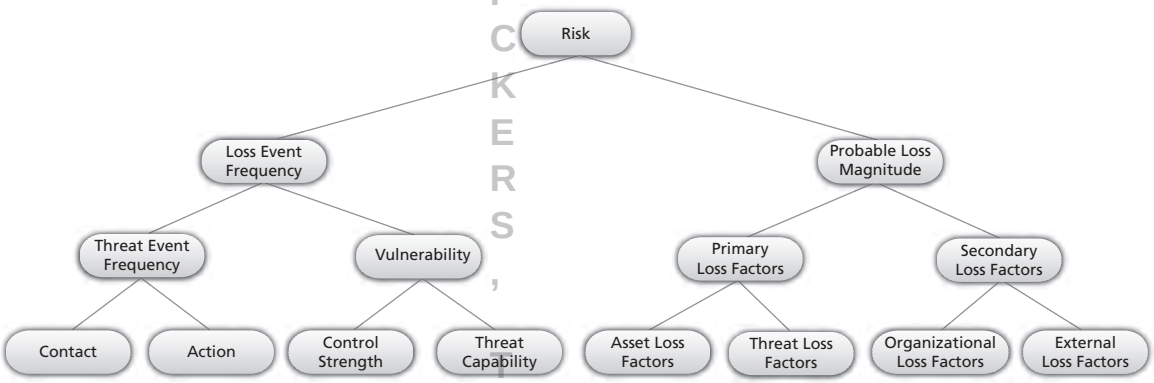

Figure 9-4 Factor analysis of information risk (FAIR)

Source: Copyright © 2014 Cengage Learning®. (Based on concepts from Jack A. Jones)[8]

ISO 27005 Standard for InfoSec Risk Management

The ISO 27000 series includes a standard for the performance of risk management: ISO 27005 (*www.27000.org/iso-27005.htm*), which includes a five-stage risk management methodology:

1. Risk assessment
2. Risk treatment
3. Risk acceptance
4. Risk communication
5. Risk monitoring and review

NIST Risk Management Model

As was briefly discussed in Chapter 8, the National Institute of Standards and Technology (NIST) has modified its fundamental approach to systems management and certification/accreditation to one that follows the industry standard of effective risk management. As discussed in "Special Publication 800-39: Managing Information Security Risk: Organization, Mission, and Information System View" *(http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf)*:

Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e., establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once determined; and (iv) monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization.

The first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations. Establishing a realistic and credible risk frame requires that organizations identify: (i) risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); (ii) risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration); (iii) risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and (iv) priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses). The risk framing component and the associated risk management strategy also include any strategic-level decisions on how risk to organizational operations and assets, individuals, other organizations, and the Nation, is to be managed by senior leaders/executives. Integrated, enterprise-wide risk management includes, for example, consideration of: (i) the strategic goals/objectives of organizations; (ii) organizational missions/business functions prioritized as needed; (iii) mission/business processes; (iv) enterprise and InfoSec architectures; and (v) system development life cycle processes.

The second component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; (iii) the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring). To support the risk assessment component, organizations identify: (i) the tools, techniques, and methodologies that are used to assess risk; (ii) the assumptions related to risk assessments; (iii) the constraints that may affect risk assessments; (iv) roles and responsibilities; (v) how risk assessment information is collected, processed, and communicated throughout organizations; (vi) how risk assessments are conducted within organizations; (vii) the frequency of risk assessments; and (viii) how threat information is obtained (i.e., sources and methods).

The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of risk assessments. The purpose of the risk response component is to provide a consistent, organization-wide, response to risk in accordance with the

organizational risk frame by: (i) developing alternative courses of action for responding to risk; (ii) evaluating the alternative courses of action; (iii) determining appropriate courses of action consistent with organizational risk tolerance; and (iv) implementing risk responses based on selected courses of action. To support the risk response component, organizations describe the types of risk responses that can be implemented (i.e., accepting, avoiding, mitigating, sharing, or transferring risk). Organizations also identify the tools, techniques, and methodologies used to develop courses of action for responding to risk, how courses of action are evaluated, and how risk responses are communicated across organizations and as appropriate, to external entities (e.g., external service providers, supply chain partners).

The fourth component of risk management addresses how organizations monitor risk over time. The purpose of the risk monitoring component is to: (i) verify that planned risk response measures are implemented and InfoSec requirements derived from/traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards, and guidelines, are satisfied; (ii) determine the ongoing effectiveness of risk response measures following implementation; and (iii) identify risk-impacting changes to organizational information systems and the environments in which the systems operate.

To support the risk monitoring component, organizations describe how compliance is verified and how the ongoing effectiveness of risk responses is determined (e.g., the types of tools, techniques, and methodologies used to determine the sufficiency/correctness of risk responses and if risk mitigation measures are implemented correctly, operating as intended, and producing the desired effect with regard to reducing risk). In addition, organizations describe how changes that may impact the ongoing effectiveness of risk responses are monitored.[9]

This approach is illustrated in Figure 9-5.

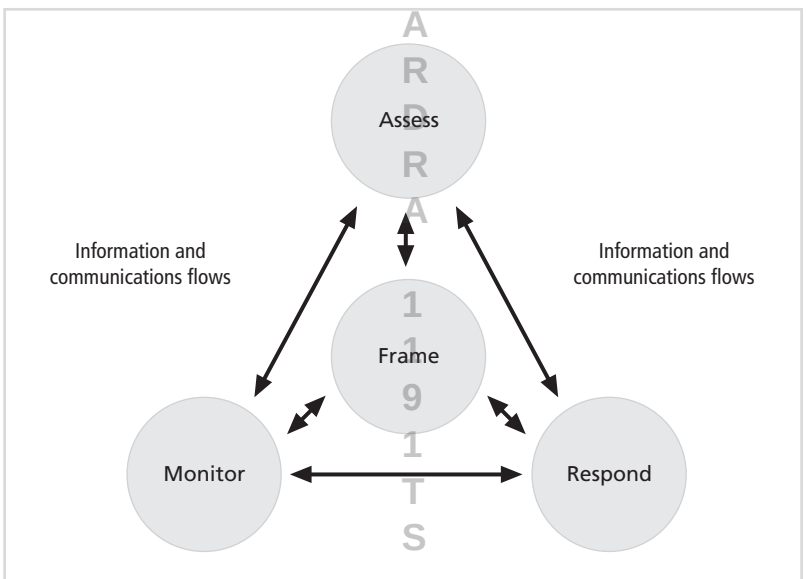

Figure 9-5 NIST risk management process

Source: NIST.[10]

Other Methods

The few methods described in this section are by no means all of the other available methods. In fact, there are two organizations that compare methods and provide recommendations for risk management tools that the public can use:

- *European Network and Information Security Agency (ENISA)*—This agency of the European Union ranks 12 tools using 22 different attributes. It also provides a utility on its Web site that enables users to compare risk management methods or tools (*www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory*). The primary risk management process promoted by ENISA is shown in Figure 9-6.
- *New Zealand's IsecT Ltd—An independent Governance, Risk Management and Compliance consultancy, IsecT maintains the ISO 27001 Security Web site at http://iso27001security.com.* This Web site describes a large number of risk management methods (*www.iso27001security.com/html/risk_mgmt.html*).

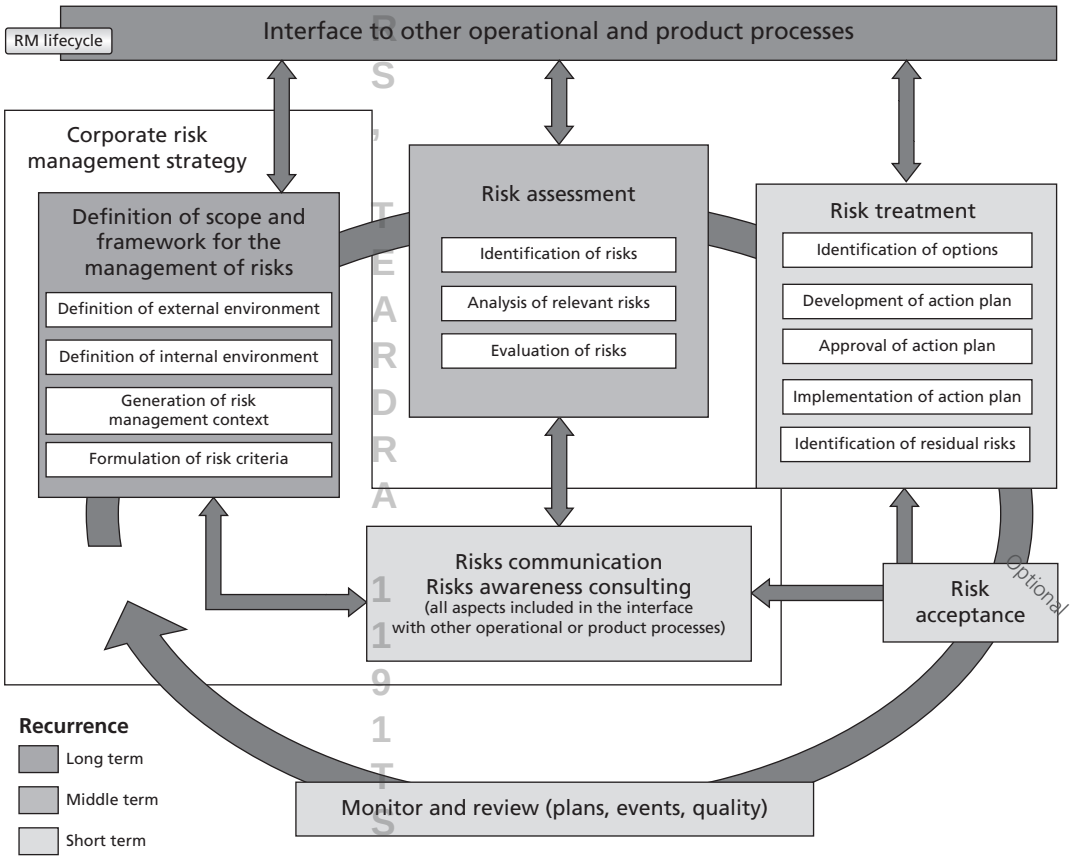

Figure 9-6 ENISA risk management process

Source: © 2005–2013 by the European Network and Information Security Agency (ENISA).[11]

Chapter Summary

- Once vulnerabilities are identified and ranked, a strategy to control the risks must be chosen. Five control strategies are: defense, transferal, mitigation, acceptance, and termination.
- Economic feasibility studies determine and compare costs and benefits from potential controls (often called a "cost-benefit analysis"). Other forms of feasibility analysis include analyses based on organizational, operational, technical, and political factors.
- An organization must be able to place a dollar value on each collection of information and the information assets it owns. There are several methods an organization can use to calculate these values.
- Single loss expectancy (SLE) is calculated from the value of the asset and the expected percentage of loss that would occur from a single successful attack. Annualized loss expectancy (ALE) represents the potential loss per year.
- Cost-benefit analysis (CBA) determines whether a control alternative is worth its associated cost. CBA calculations are based on costs before and after controls are implemented and the cost of the controls. Other feasibility analysis approaches can also be used.
- Organizations may choose alternatives to feasibility studies to justify applying InfoSec controls, including: benchmarking with either metrics-based measures or process-based measures; due care and/or due diligence; best security practices up to and including the near-mythic gold standard; and/or baselining.
- Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the trade-offs between perfect security and unlimited accessibility. Residual risk is the amount of risk unaccounted for after the application of controls.
- It is possible to repeat risk analysis using estimates based on a qualitative assessment. The Delphi technique can be used to obtain group consensus on risk assessment values.
- Once a control strategy has been implemented, the effectiveness of controls should be monitored and measured.
- Alternative approaches to risk management include the OCTAVE Method, the Microsoft risk management approach, ISO 27005, the NIST risk management approach, and FAIR.

Review Questions

1. What is competitive advantage? How has it changed in the years since the IT industry began?
2. What is competitive disadvantage? Why has it emerged as a factor?
3. What are the five risk control strategies presented in this chapter?
4. Describe the strategy of defense.
5. Describe the strategy of transferal.
6. Describe the strategy of mitigation.

7. Describe the strategy of 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?
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 (Asset value: $1,200,000 in projected revenues)		
Threat Category	**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 shown in the table that is included in Exercise 1? For each row in the table, describe the process of determining the cost per incident and the frequency of occurrence.
3. How could we determine EF 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 (Asset value: $1,200,000 in projected revenues)				
Threat Category	**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 that 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
   - Cisco firewall (other than residential models from LinkSys)
   - Tripwire host-based IDS for 10 servers

- Java programming continuing education training program for 10 employees
- Checkpoint Firewall solutions

Closing Case

Mike and Iris were reviewing the asset valuation worksheets that had been collected from all the company managers.

"Iris," Mike said after a few minutes, "the problem, as I see it, is that no two managers gave us answers that can be compared to each other's. Some gave only one value, and some didn't actually use a rank order for the last part. In fact, we don't know what criteria were used to assess the ranks or even where they got the cost or replacement values."

"I agree," Iris said, nodding. "These values and ranks are really inconsistent. This makes it a real challenge to make a useful comprehensive list of information assets. We're going to have to visit all the managers and figure out where they got their values and how the assets were ranked."

Discussion

1. If you could have spoken to Mike Edwards before he distributed the asset valuation worksheets, what advice would you have given him to make the consolidation process easier?
2. How would you advise Mike and Iris to proceed with the worksheets they already have in hand?

Ethical Decision Making

Suppose Mike and Iris make a decision to simply take the higher of each of the values without regard to how the values were determined by the person who made the initial assessment. Then, they determine- their own rankings among all of the compiled assets. When the list is later included in the planning process, they represent it as being authoritative since it came from "all of the managers."

Is this method, even if it is faster and easier, an ethical way to do business? Why or why not?

Endnotes

1. Peters, Thomas, and Robert Waterman. *In Search of Excellence: Lessons from America's Best-Run Companies*. New York: Harper and Row, 2004.
2. Anderson, James. "Panel Comments at 2002 Garage Technology Venture's State of the Art Conference," 2002.
3. "Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments." *National Institute of Standards and Technology (NIST)*, September 2012.
4. "Ready Business Mentoring Guide Working with Small Businesses to Prepare for Emergencies" *FEMA*. Accessed December 17, 2012 @ *www.ready.gov/document/ready-business-mentoring-guide-working-small-businesses-prepare-emergencies*.

5. Avolio, Frederick. "Best Practices in Network Security." *Network Computing*, March 20, 2000. Accessed March 19, 2013 @ *www.networkcomputing.com/1105/1105f2.html*.
6. Mann, Thomas. "Politics Is Often Defined as the Art of the Possible." Speech in the Library of Congress, Washington, DC, May 29, 1945. Bismark, Otto Von. Interview (11 August 1867) with Friedrich Meyer von Waldeck of the St. Petersburgische Zeitung; reprinted in *Fürst Bismarck: neue Tischgespräche und Interviews*, Vol. 1, p. 248.
7. "Microsoft Security Risk Management Guide." *Microsoft.com*, March 15, 2006. Microsoft. Accessed June 13, 2013 @ *http://technet.microsoft.com/en-us/library/cc163143.aspx*.
8. Jones, J. "An Introduction to Factor Analysis of Information Risk (FAIR): A Framework for Understanding, Analysing, and Measuring Information Risk." (2005). Accessed July 1, 2013 @ *www.riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf*.
9. "SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View." *National Institute of Standards and Technology*, March 2011. Accessed December 17, 2012 @ *http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf*.
10. "SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach." National Institute of Standards and Technology, February 2010. Accessed July 1, 2013 @ *http://csrc.nist.gov*.
11. ENISA. Accessed July 25, 2013 @ *www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process*.