Chapter 1

Introduction

1.1 The Role of the Information Security Manager

For those responsible for information security within their organization there are a clear set of responsibilities. These include

- Preventing loss, fraud, and sensitive data breaches
- Demonstrating regulation compliance
- Managing security policies
- Ensuring business continuity
- Planning incident and disaster response, and
- Prioritizing security initiatives

There can be some debate as to the inclusion of these responsibilities with all information security managers or officers as organizational structures may place responsibility of fraud or business continuity in other departments, but one responsibility remains clear. The senior most security person must be able to determine, from the myriad of available security projects, the most advantageous projects to initiate.

Despite the structural differences between organizations, the threat or regulation environment, or even across economic conditions, there is always a limit to the available funding and staff required to perform security initiatives. It is not enough to know a set of desired security projects for the organization to improve its security posture. Security managers need to be able to justify their next project and defend these decisions.

There are several approaches to identify and prioritize the security initiatives to be funded within your organization. Each of these approaches is discussed briefly below.

1.1.1 Audit as a Driver for Security Initiatives

When the results and recommendations of an information security audit is the primary driver for determining the next security initiative in an organization, the organization has no clear security strategy. No doubt the findings of an information security audit need to be addressed but reliance on these results as the guide to improving the organization's security posture is shortsighted. Audits by their nature are reviews of what have been done against policies and procedures that have been established. A security strategy based only on what the auditors find will be in a constant state of catch-up. Moreover, improvement priorities will be audit-based, which is limited to the threats to our organization that we already know about and have written policies and procedures to address.

1.1.2 Technology as a Driver for Security Initiatives

Another approach to developing a security strategy that is often arrived at by default is a technology-based security strategy. It is clear that technologists and vendors have been able to supply the industry with a steady stream of improvements and new security products. Many times these products are just what an organization needs to enact protection measures for their assets. However, a security strategy that relies too heavily on technology to dictate the security solutions will find the administrative and physical areas of their protection measures lacking.

1.1.3 Compliance as a Driver for Security Initiatives

Information security regulations and industry requirements seem a natural place to start when creating a security strategy for an organization. However, these requirements are merely a portion of the security requirements to be addressed for the organization. An organization needs to address customer and business mission requirements as well. Organizations that take a compliance-driven strategy to security may find themselves battling the silo approach (e.g., HIPAA security effort, PCI DSS effort, Privacy effort, etc.). Reliance on compliance regulations leads to the inevitable discovery that regulations do not provide adequate guidance for implementation. Furthermore, it is difficult to plan for the next iteration of changes to regulations.

1.1.4 Security Risk as a Driver for Security Initiatives

Even though each of these approaches offers some benefit, a more complete security strategy can be created based on an analysis of security risk. It is risk to the organization's assets that needs to be addressed. The best way to address it is to first measure it. As clear as this statement seems it is still surprising that an information security risk assessment is not always the driver for creating a security strategy.

It is useful to ask the following question of security managers (or have them ask it of themselves):

> *Given your limited resources, are you confident that your initiatives are addressing the largest security risks to your organizations assets?*

At first blush this seems an innocent enough question and is often answered quickly in the affirmative. Following this question with a more probing question often gives the security manager pause:

> *How do you demonstrate that your initiatives are addressing the largest security risks to your organizations assets to management?*

The reason the question above is a more difficult question is that is seems hard to demonstrate that the limited resources are being utilized to address security risk efficiently if security risk is not measured or not measured adequately. With so much riding on the results of an information security risk assessment it is important that they are done right.

1.2 Ensuring a Quality Information Security Risk Assessment

If the security manager has properly aligned his security strategy with the results of an information security risk assessment then he can demonstrate that the planned security initiatives are addressing the largest security risks to the organization. At this point, when a security risk assessment is used as the basis for security decisions, the quality of the information security risk assessment becomes critical. A weak security risk assessment method can lead to false conclusions and bias results and eventually lead to significant planning errors and increased security risk.

The importance of the information security risk assessment and a quality method for performing it is the reason for the creation of this book (Figure 1.1). Information security risk assessments should not be merely performed to check a box or to satisfy a regulatory requirement. Instead an information security risk assessment should be performed in a professional manner that provides accurate results.

1.3 Security Risk Assessment

Security risk assessment the value of information assets, measures the strength of the overall security program, and provides the information necessary to make planned improvements based on information security risks. The security risk assessment is

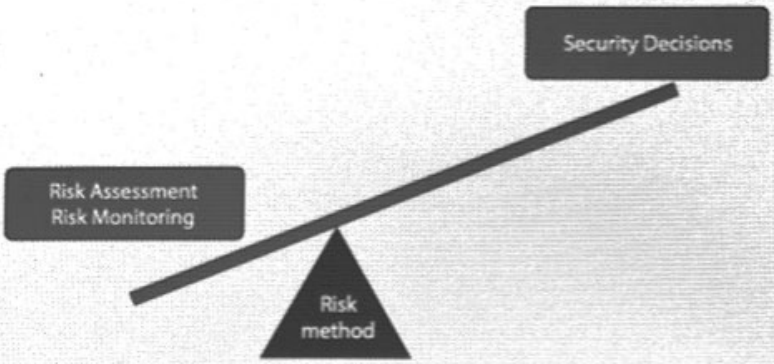

Figure 1.1 Importance of Security Risk Assessment method. When a security risk assessment is used as the basis for making security decisions in the organization, the risk method is highly leveraged. Weaknesses in the risk assessment method can eventually lead to planning errors and increased security risk.

the tool of senior management that gives them an effectiveness measurement of their security controls and an indication of how well their assets are protected.

1.3.1 The Role of the Security Risk Assessment

A security risk assessment is an important element in the overall security risk management process. Security risk management involves the process of ensuring that the security risk posture of an organization is within acceptable bounds as defined by senior management. There are four stages of the security risk management process: security risk assessment; test and review; security risk mitigation; and operational security (see Figure 1.2).

- Security Risk Assessment—This is an objective analysis of the effectiveness of the current security controls that protect an organization's assets and a determination of the probability of losses to those assets. A security risk assessment reviews the organization's threat environment, the asset values, the system's criticality, the security controls' vulnerabilities, and the expected losses impact, and also provides recommendations for additional controls to reduce security risk to an acceptable level. Based on this information, the senior management of the organization can determine if additional security controls are required.
- Test and Review—Security testing is the examination of the security controls against the security requirements. The need for additional security controls to obtain an acceptable level of security risk is determined during the security risk assessment. Security testing can be applied to any number of or subset of security controls, such as physical controls testing (e.g., doors, access control), vulnerability scanning (e.g., external interfaces), or social engineering

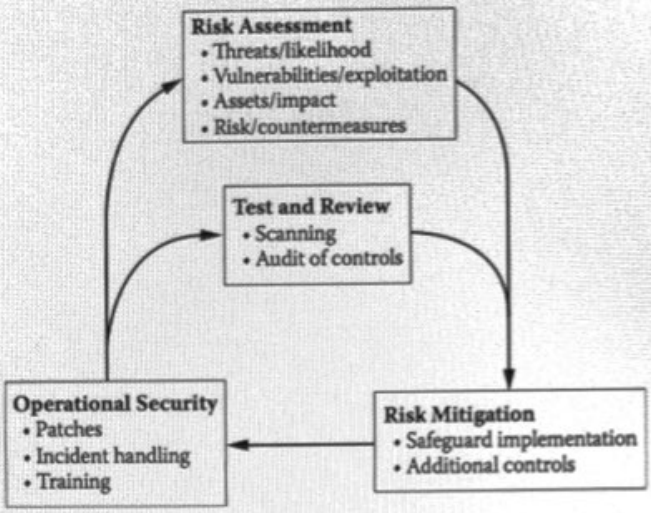

Figure 1.2 The role of the security risk assessment. Security risk assessments play a critical role in the security management process, providing information on the threats, assets, and security risks to an organization.

(e.g., user behavior). Typically, security testing is performed more frequently than security risk assessments.

- Security Risk Mitigation—Either the reported security risks are accepted or security risks to an organization's assets are reduced through the implementation of new security controls or the improvement of existing controls. Security risk assessments provide information to allow the senior management to make security risk-based decisions for the development of new controls or the expenditure of resources on security improvements of existing controls. Security test and review efforts provide information on how to keep existing controls up to date. Security risk can be mitigated through corrections and additional controls, accepted or transferred.
- Operational Security—The implementation and operation of most security controls are performed by operational personnel. Daily and weekly activities such as applying patches, performing account maintenance, and providing security awareness training are essential for maintaining an adequate security posture.

1.3.2 Definition of a Security Risk Assessment

The security risk assessment takes on many names and can vary greatly in terms of method, rigor, and scope, but the core goal remains the same: assess the security risks to the organization's information assets. This information is then used to determine how best to mitigate those security risks and effectively preserve the organization's mission.

There is no shortage of definitions for a security risk assessment (and many other closely associated names). Many of these definitions are overly complex or may be specifically geared to an industry segment such as the federal government. For example, the National Institute of Standards and Technology provides two alternative definitions for the term *security risk assessment*. One definition, found in the NIST "Risk Management Guide" (2002), states that security risk assessment is "the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact." Yet another definition found in the NIST "Guide for Security Certification and Accreditation" expands the definition to describe the process required for the certification and accreditation of federal systems. It reads as follows:

> The periodic assessment of risk to agency operations or assets resulting from the operation of an information system is an important activity required by [Federal Information Security Management Act of 2002] FISMA. The risk assessment brings together important information for agency officials with regard to the protection of the information system and generates essential information required for the security plan. The risk assessment includes: (i) the identification of threats to and vulnerabilities in the information system; (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image, or reputation) or agency assets should there be a threat exploitation of identified vulnerabilities; and (iii) the identification and analysis of security controls for the information system.

Other uses of the term *risk assessment* are geared toward a specific use, such as complying with the Sarbanes-Oxley Bill. The IT Governance Institute defines *risk assessment* as the identification and analysis by management of relevant risks to achieve predetermined objectives, which form the basis for determining control activities.[3] Furthermore, the IT Governance Institute recognizes that risk assessments may be performed at the company level or at the level of an individual activity. A risk assessment performed at the company level is concerned with the overall risks to the company. Such a risk assessment would require senior-level management oversight, the integration of a strategic plan for measuring and controlling risk throughout the company, and, of course, the assessment of information technology risks. A risk assessment performed at the activity level would encompass formalized or built-in risk assessments in individual control activities. Examples of activities include change-management control, application testing, and account creation, maintenance, and termination.

The ISO 27001/2 takes an integrated approach to security management and recognizes the value of security risk assessments in that process. The basic structure of security management involves selecting security requirements, assessing the

risks, and selecting controls. The security risk assessment is central to this approach, as it assesses the risks that the security requirements may not be met and provides the basis for a risk-based decision for selecting security controls.

The ISO 27001/2 defines *risk assessment* as the "systematic consideration of the business harm likely to result from a security failure... and the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented" (ISO, 2000).

In all the regulations, guidelines, and standards, *security risk assessment* has been defined in numerous ways. Some definitions are more detailed than others in terms of how an assessment is performed. Some definitions focus on the result of the assessment, while others focus on the approach. For our purposes, a simpler *security risk assessment* definition is needed to cover any such approach or detail. Because this book will discuss the various methods of performing a security risk assessment, the definition used here is designed to fit all such methods. For the purposes of this book, *security risk assessment* if defined as follows:

> Security Risk Assessment—A probability determination of asset losses based on asset valuation, threat analysis, and an objective review of current security controls effectiveness.

1.3.3 The Need for a Security Risk Assessment

Aside from being required, a security risk assessment is an essential element of any corporation seeking to protect its information assets. A security risk assessment has the following benefits to an organization.

1.3.3.1 Checks and Balances

A security risk assessment provides a review of the organization's current implementation of information asset protection. The work of the information security officer and the security operations staff should be assessed by an objective party to determine the adequacy of the program and to note areas for improvement. Those who have architected the security program and those who are administering security controls are too close to the decisions that have been made and are not likely to be able to provide an objective analysis. (More on this in Section 12.1.3 Project Resources.)

1.3.3.2 Periodic Review

Even the most carefully constructed information security program requires a periodic review. A periodic review of an information security program can provide a measure of the effectiveness of the program and information necessary to properly adjust the program for the changing threat environment and business mission.

Many elements of an information security program require periodic review to measure their effectiveness. For example, the security awareness training program should be reviewed to measure and improve its effectiveness. Such measurements should not be limited to student evaluations of courses delivered, but the actual security awareness that has been instilled into the culture of employees and others who have access to an organization's information assets. Additional measurements could be obtained through physical inspections, policy quizzes, and social-engineering experiments, to name a few.

Moreover, the landscape in which an information security program is developed is constantly changing. Threats to the organization's information assets change as technology advances, information is promulgated, skills (or tools) are acquired by would-be intruders, and interfaces to the organization's assets increase. Prior to widespread knowledge, tools, and tutorials, an SQL (Structured Query Language) injection attack on a database required the skills of a determined intruder. Nowadays, less skilled and more abundant script-kiddies possess the ability to launch the same attack through tools circulated freely on the Internet.

Similarly, several years ago many organizations could state, with reasonable confidence, that they were aware of and controlled all interfaces to their networks. However, if an organization lacks the proper controls, the introduction of cheap wireless routers that can be added to connected laptops can render such a statement wishful thinking.

Lastly, your organization's mission may have changed since information security controls were first devised. Changes in mission can change everything from the reclassification of sensitive data and the addition of partners and extended networks to the development of new systems, connections, and security risks. Without a periodic security risk assessment, an organization's information security program would remain stagnant while threats, attacker skills, and business missions change. The result would be a steady decline of the effectiveness of the information security program and an increased risk, as illustrated in Figure 1.3.

1.3.3.3 Risk-Based Spending

Resource allocation can be based on security risk to assets. Organizations have limited resources to address their information security issues. If a security risk assessment is not performed, the organization does not have an understanding of the security risks to its information assets. In the absence of security risk information, resources are allocated on a variety of other factors, including convenience, existing familiarity or skill, or simply interest.

When deciding how to spend the information security budget, the decision makers may choose the latest gadgets offered by vendors who have an existing relationship to the organization. Similarly, the decision makers may choose to expand the capabilities of the organization within an area with which they are familiar. For example, the information security manager may be an expert in configuring

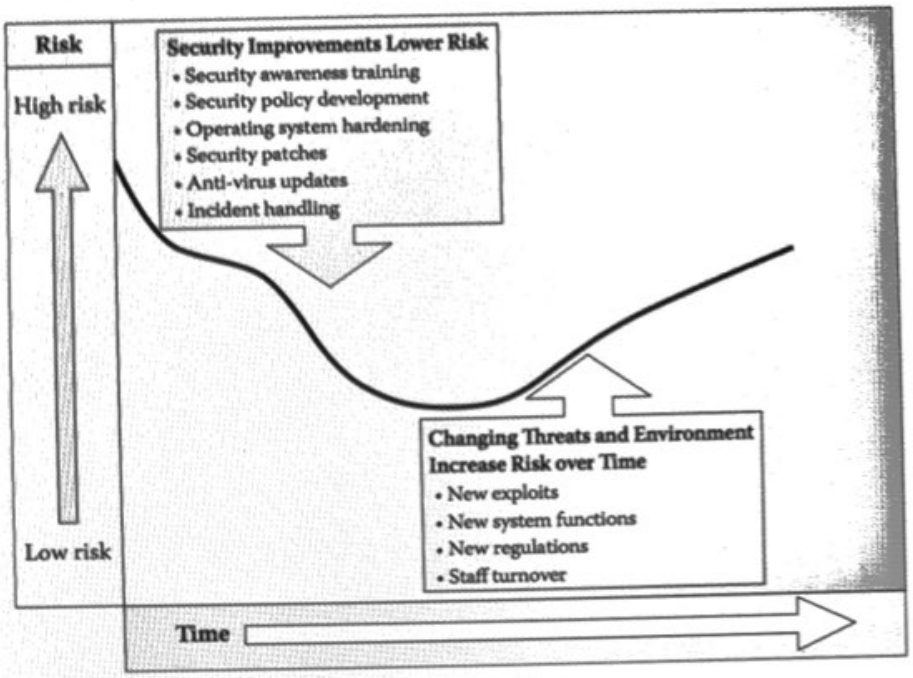

Figure 1.3 The eroding security posture. Applying security improvements such as security awareness training and security patching can lower the security risk of an information system, but the changing threats and environment will erode the security posture over time.

perimeter devices to filter the content of outgoing messages. There may be exciting advances within this field. It would be natural for this manager to be drawn toward pursuing the integration of such advances into the existing information asset control architecture. Lastly, the decision makers may simply be swayed by "cool" technology. While many of these controls will likely improve the security posture of the organization, they may not deliver the best "bang for the buck."

Consider an organization that currently has an inadequate security awareness program and lacks the proper information security policies. Recognizing that security programs break at the weakest link, it is not a stretch to imagine that a security risk assessment would point out that the lack of an adequate security awareness program and security policies poses the greatest security risk to an organization's assets. However, without a consideration of how security controls would ultimately reduce the overall security risk to an organization, other more familiar or interesting controls will likely receive funding over such administrative controls. When is the last time you remember a security professional being interested in developing a security awareness program?

1.3.3.4 Requirement

A security risk assessment is a required element of a security program according to multiple information security regulations. These regulations include HIPAA, GLBA, NERC (North American Electric Reliability Corporation), and CIP (Critical Infrastructure Protection) Cyber Security Standards, ISO 27001/2, OMB A-130 (Office of Management and Budget), FISMA (Federal Information Security Management Act), and many others. If for no other reason, many organizations obtain a security risk assessment simply because it is required.

1.3.4 Security Risk Assessment Secondary Benefits

Aside from the obvious benefits mentioned in Section 1.4.3, a security risk assessment may provide some secondary benefits to an organization as well. Among those benefits are the transfer of knowledge from the security assessment team to the organization's staff, increased communications regarding security among business units, and increased security awareness within the organization. In addition, the results of the security risk assessment may be used as a measure of the security posture and compared to previous and future results.

There is an expectation that the members of the security assessment team will be experts in the field of information security. As we shall discuss in this book, the ability to observe, estimate, assess, and recommend is largely based on having experience with security mechanisms, how they work, and how they fail. An experienced security risk assessment team will be able to apply that knowledge to specific implementations of security mechanisms within the unique environment of the organization. Throughout the data-gathering process and the draft and final security risk assessment report, the experience of the team will be shared with the organization. Many of the insights shared may prove valuable to the organization and would not otherwise have been gained.

The fact that a security risk assessment team is focused solely on the security risks to the organization requires that the interaction of security mechanisms between business units need to be addressed—perhaps for the first time. The security risk assessment may allow for or even force a security discussion among the business units. For example, when assessing the effectiveness of termination procedures, the legal, human resources, physical security, and information technology departments will all need to work together to ensure an effective approach and execution of these procedures.

A security risk assessment includes many activities that may test the security awareness of the employees within the organization. A security risk assessment will include physical security walk-throughs, checks on perimeter controls, and interviews with employees and key personnel, and it may include social engineering. All of these activities will result in an indication of how effective security awareness training is within the organization. Making specific results known to the employees of the organization will increase the overall security awareness. For example, if

the security risk assessment team was able to "piggyback" through physical access controls (e.g., trailing behind someone who has swiped a badge to open a door), consider letting the organization's employees know the results of those tasks. This will increase their awareness that such breaches can actually occur and that it is their responsibility to help enforce current policies.

The security risk assessment should conclude with a list of security risks to the organization's assets and an indication of the organization's overall security posture. These results can be compared to the previous and future results to assist in tracking the progress of the information security program. Organizations that consistently find that their security posture indicates that they are taking a larger security risk than they are comfortable with should consider increasing the resources allocated to information security. The organization should also ask the security risk assessment team for a comparison of the organization's security program with those of similar organizations. As mentioned previously, the members of the security risk assessment team will have experience with other organizations and should be able to provide a rough comparison of how this organization measures up to its peers in the industry.

1.4 Related Activities

There is much confusion surrounding the terms used to describe an assessment of the security mechanisms within an organization. Although there are clearly different approaches, objectives, and levels of rigor within various assessments, there does not seem to be a well-understood and accepted method for describing each of these assessments. For the purposes of this book and for clearly describing our topic, the following descriptions are offered.

All of the services listed in Tables 1.1 and 1.2 are related but should not be confused with a security risk assessment. A security risk assessment and the services described may be performed by professionals with similar credentials who use similar tools and checklists. However, a security risk assessment is differentiated from the other services in that only a security risk assessment takes a risk-based approach at identifying vulnerabilities within the organization's security controls. Only a security risk assessment provides recommendations for improvement based on the actual and perceived security risks to the organization.

1.4.1 Gap Assessment

A gap assessment is the comparison between what exists within a corporation and what is required. Typically, gap assessments are associated with specific criteria, e.g., HIPAA Gap Assessment or ISO 27001/2 Gap Assessment. These assessments compare the existence of security policies, procedures, and mechanisms, along with activities (which may include a security risk assessment), against the required

Table 1.1 Addressing Security Risks

Security Program Elements	*Vulnerability Scan*	*Penetration Test*	*Security Risk Assessment*
Organization			Organizational effectiveness analysis
Policy and procedure			Security policy and procedure review
Architecture			Security architecture review
Applications		Common mistakes, perform ad hoc testing, side effects	Common mistakes, perform ad hoc testing, side effects
External I/F	Scan for known vulnerabilities	Scan for known vulnerabilities	Scan for known vulnerabilities
Internal I/F	Scan for known vulnerabilities	Scan for known vulnerabilities	Scan for known vulnerabilities
Security awareness		Social engineering	Assess security awareness, social engineering
External modems		War dialing	War-dialing configuration review

Note: Vulnerability scans and penetration testing provide a review of some of the elements of a security program. However, many key elements of the security program are left unchecked. The security risk assessment provides a complete review of an organization's security program.

security policies, procedures, mechanisms, and activities dictated in the HIPAA regulation or in the ISO 27001/2 guidelines. There is no measure of security risk associated with this assessment; it is merely a review of what exists against an interpretation of what the regulation or guideline requires.

A gap assessment is performed at the beginning of the organization's compliance pursuit with a standard or regulation. Since the gap assessment will result in a list of "gaps" or things that need to be done prior to declaring compliance, these assessments do not require verification of findings. If an interview with key personnel and a review of the materials reveal that the security awareness program is

Table 1.2 Security Assessment Definitions

Term	*Definition*	*Purpose*
Gap assessment	A review of security controls against a standard	To provide a list of controls required to become compliant
Compliance audit	Verification that all required security controls are in place	To attest to an organization's compliance with a standard
Security audit	A verification that specified security controls are in place	To attest to an organization's adherence to industry standards
Penetration testing	A methodical and planned attack on a system's security controls	To test the adequacy of security controls in place
Vulnerability scanning	An element of penetration testing that searches for obvious vulnerabilities	To test for the existence of obvious vulnerabilities in the system's security controls

Note: There are a great many different ways to review the security controls of an organization. Terms such as *assessment, audit,* and *test* are commonly used as synonyms, yet it is important to understand the distinctive use and limitations of these industry terms.

adequate, then the assessment team need go no further with this line of review. The point is to efficiently reach the point where the organization knows what the compliance project entails. An efficient gap assessment helps them get a quicker start. The organization being assessed should realize that deceiving the gap assessment team will only result in an inaccurate compliance plan.

1.4.2 Compliance Audit

When the time comes to attest to the organization's compliance with a regulation or a standard, a more in-depth review is required. This review requires that all findings be verified. The same interview and review of the security awareness training program would be followed up with review of a sample of employee training records and interviews with some employees. A compliance audit still does not result in a measure of the security risk to the organization's assets. A compliance audit is an objective review of the organization's compliance with a security standard, such as HIPAA Privacy and Security Rule, Gramm-Leach-Bliley Act, ISO 27001/2, or other regulations and standards that specify security controls that need to be in place.

1.4.3 Security Audit

A security audit, also called a security controls review, is a verification that the security controls that have been specified are properly implemented. Proper implementation may be further defined in existing organizational security policy and procedures or within industry standards, such as COBIT, ISO 27001/2, and others. Depending on the standards, these security audits can be quite rigorous and even involve statistically relevant sampling techniques and complete verification of all findings.

One thing that is common to all security audits is the overhead implicit in the assessment to ensure consistency with the standard. Many information security standards have associated assessment standards that specify the degree to which the assessor must analyze the data, sample the controls, and complete other such requirements. Many information security standards also require the assessors to obtain the proper credentials or require the assessor's company to be an auditing firm. While these requirements ensure consistency, they also add significantly to the cost of the audit. In most cases a "security audit" would cost far more than a security risk assessment.

The major differences here are level of rigor and formality of the statement. For example, a security audit performed under SAS No. 70[4] is said to be an "attestation" [16]. This means that a certified public accountant (CPA) has expressed a conclusion about the reliability of a written statement that is the responsibility of someone else. There are two key elements of this definition. First, a CPA provides a conclusion as to the reliability of a written statement. Security audits incur significant overhead, since they must be overseen by a licensed CPA, the reports are issued by a licensed CPA firm, and the report is a formal input into the accounting process. Second, the written statement is a statement regarding the presence of reasonable assurance that control objectives are met. Control objectives are statements of the intended result or purpose achieved by implementing security controls. These statements are tailored to the organization and the security it is intended to provide.

It is important to understand that, because of the way it is structured, the SAS 70 audit (and most standards-driven audits) does not perform a security risk assessment. These security audit methodologies review an organization against a standard and do not provide an analysis of the effectiveness of the current security controls. Instead, these security audits review the current security controls against a standard or a statement produced by the organization being assessed.[5]

1.4.4 Vulnerability Scanning

Vulnerability scanning is the testing of the external or internal interfaces of a system in order to identify obvious vulnerabilities. At a bare minimum, this service involves running a vulnerability scanning tool to test the known interfaces to the system and providing the tool-generated report. These tools are constantly updated with the knowledge of common system vulnerabilities. A more in-depth vulnerability scanning service would perform additional analyses and checks to remove

false positives generated by the tool. A false positive is an indication by a security engineer, using personal knowledge of the system, a vulnerability identified by the tool does not really exist. These false positives are typically quite numerous in tool-generated reports.

1.4.5 Penetration Testing

Also called ethical hacking, white-hat hacking, security testing, and attack and penetration studies, this service is provided by an objective team who attempt to penetrate the defenses of an organization in order to demonstrate the effectiveness of the current controls. A vulnerability scan is typically performed as the first stage of a penetration test. The vulnerability scan would provide one source of information to the security testers for their use in attempting to penetrate the system. Penetration testing actually comprises several elements, including vulnerability scanning, ad hoc testing, war dialing, social engineering, and other techniques. These elements can also be performed as a stand-alone test or as part of the security risk assessment data-gathering phase.

1.4.6 Ad Hoc Testing

Whereas vulnerability scans test for obvious vulnerabilities, ad hoc testing is a search for less obvious vulnerabilities. This type of testing must be performed by experts who use various techniques and knowledge gained from years of experience. This is more of an art than a science, but methods and some tools are available or developed in-house to assist in the process.

1.4.7 Social Engineering

This type of testing involves an assessment of the security training, policies, and procedures of the organization by attempting to gain unauthorized access through the human element. Social engineering by its nature is ad hoc and varies each time. Examples of this testing include gaining unauthorized physical access through "piggybacking," obtaining user identification and passwords through the help desk, and gaining unauthorized information through temporary or new employees. Basically, social engineering involves gaining the confidence of authorized users in order to obtain sensitive information or gain access.

1.4.8 War Dialing

Another way of threatening an organization's assets is to gain access to its information systems or control systems through unprotected modems. This method is referred to as *war dialing*. A war-dialing effort consists of identifying all organizational phone numbers that have modems attached (footprinting), determining the

vulnerabilities of these various modems (preparation), and finally gaining access to the organization's systems through vulnerable modems. Systems targeted include not only information systems but also environmental systems such as the High Volume Air Conditioning (HVAC), security systems, and telephone systems (or private branch exchanges—PBXs).

1.5 The Need for This Book

The proliferation of information security and privacy laws, not to mention lawsuits, has mandated that businesses perform information security risk assessments. Five to ten years ago, an analysis of the effectiveness of security controls was rarely performed outside of government agencies and organizations with the highest security concerns. Now most organizations are incorporating a security risk assessment into their information security programs as a way to continually improve their controls and remain compliant with information security regulations. At the same time, the demand for security risk assessments has exploded, but the supply of experienced information security engineers to perform them has not kept up with the demand.

In order to provide relief to this situation, there have been several promising advances in the area of security risk assessments. There are many sources of information that describe various information security risk assessment processes. These resources include (a) general security program guidance, which includes discussions on security risk assessments; (b) descriptions of security risk assessment methodologies; and (c) information on security risk assessment tools. These resources are useful to most information security professionals involved with commissioning or performing a security risk assessment.

General Security Program Guidance—Groups such as ASIS International and federal agencies such as NIST have provided general guidance that covers some aspects of performing security risk assessments. Below are a few examples.

- NIST Special Publication 800-12: *An Introduction to Computer Security: A NIST Handbook* (1995)—This publication provides an excellent overview of the security risk management process, which includes security risk assessment, security risk mitigation, and uncertainty analysis [15]. Chapter 7 of the handbook provides a general description of the objectives and the processes involved in security risk management. This handbook is useful to anyone wanting to understand the various processes in computer security, their objectives, and how they interrelate. The coverage of security risk assessment is at a high level, but it provides the reader with a strong explanation of the phases of the process in terms of how the phases work together to provide management with the information required to make an informed decision regarding the security risk decisions for the organization.

- NIST Special Publication 800-30: *Risk Management Guide: Recommendations of the National Institute of Standards and Information Technology Systems* (2002)—This publication provides a detailed discussion of a nine-step process for security risk assessments. The nine-step process includes system, threat, and vulnerability identification; control and impact analysis; likelihood and security risk determination; control recommendation; and results documentation. For each of these steps, the NIST publication provides a discussion of the relevant point, offers some advice, and references several other useful sources of information. This publication offers a simplistic approach to calculating the security risk level for each system procedure/vulnerability pair. The publication offers a list of general categories of security risk prevention, detection, and recovery controls and advice on cost–benefit analysis.
- ASIS International: *The General Security Risk Assessment Guideline*—This guideline was published to obtain a consensus regarding general practices for performing security risk assessments (2002). The document outlines a seven-step process that comprises system and asset identification, specification of vulnerabilities, determining security risk probabilities and event impact, developing security risk mitigation options, studying the feasibility of options, and performing a cost–benefit analysis. The bulk of the ASIS security risk assessment guideline is the practice advisories contained in "Appendix I: Qualitative Approach." These practice advisories include several examples to help illustrate the seven-step process. The ASIS guideline also provides many useful references.
- Security Risk Assessment Methods—Other groups and individuals, such as Carnegie Mellon University, have produced general security risk assessment models and methods that are designed to be used in the performance of a security risk assessment. For a more complete discussion of security risk assessment methods, see Chapter 13.
- Security Risk Assessment Tools—There is even a good set of security risk assessment tools available to those looking at providing a security risk assessment service or with performing a security risk assessment within their own organizations. Security risk assessment tools include everything from simple checklists to complex software packages. For a more complete discussion of security risk assessment methods, see Chapter 13.

However, none of these resources is able to provide an explanation of the complete and detailed security risk assessment process sufficient to assist an information security professional in actually performing the work.

Although many information security risk assessment products, services, and approaches exist, little guidance is available to those who need to perform them. For all the literature that exists on the topic, there still is little available advice or guidance that tells the security practitioner how to get started, how to behave, how

to present the results, or how to acquire any one of several dozen skills required to actually perform a security risk assessment. There is a frustration commonly experienced by information security professionals when attempting to perform a security risk assessment. Although existing material describes in detail the components of a security risk assessment, little information is available on how to execute those components. The "why" and the "what" are well explained, but there seems to be no information on the "how."

For example, most guidance currently available outlines the step in which the security risk assessment team must determine the impact of an event. The available guidance provides the structure for a security risk assessment team to work within by informing that losses may be direct and indirect, by emphasizing that the team must understand the business mission and consider the various security policies that could be threatened, and even by giving sample qualitative categories and descriptions such as "low," "medium," and "high." However, none of the guidance documents tells the team exactly how to come up with the impact classification for each of the security risk statements. No examples are given. No guidelines on ideal team size or decision techniques. No specific guidance on how to actually get this job done exists. Until now, that specific guidance has only been developed by experienced information security professionals and absorbed by less experienced team members during an actual engagement.

This book will attempt to document just that experience and advice. By providing real examples, step-by-step descriptions, checklists, decision techniques, and other tricks of the trade, this book will provide a detailed insight into precisely how to conduct an information security risk assessment from a practical point of view.

1.6 Who Is This Book For?

This book is designed and intended for anyone who wants a more detailed understanding of how to perform an information security risk assessment. The audience for this book includes security professionals who want a more in-depth understanding of the process of performing a security risk assessment and for security consumers who want a better understanding of what goes into completing a security risk assessment project.

Security professionals will benefit from this book, as the information will help them to become more valuable members of—or perhaps even to lead—a security risk assessment team. The information in this book contains practical real-world advice that will help develop the experience of the security professional reader.

Security consumers will benefit from this book by having greater insight into the security risk assessment process. The process descriptions and examples in this book will give the security consumer a more in-depth understanding of the entire process. Enlightened security consumers are then better educated to negotiate the

scope and rigor of a security assessment, interface with the security assessment team more effectively, provide insightful comments on the draft report, and have a greater understanding of the final report recommendations.

As a result of reading and using this book, it is envisioned that the reader will save both time and money. Students of this text can expect to save time since they will spend less time figuring out what activities to do next and precisely how to perform them. In addition, the charts, checklists, examples, and templates included in this text can speed up the process of data gathering, analysis, and document development for the security risk assessment effort.

It is also expected that students of this text can save money as well. In the world of information security consulting, time is money. This text is designed to increase the quality of a consultant's product and reduce the amount of effort it takes to create that product. Such advances can lead to consultants providing a better, less expensive service for their customers and perhaps even making a larger profit in the process.

The security service consumer will benefit from reading this book as well. In addition to being the recipient of better, cheaper, faster security risk assessments, security consumers who have a more in-depth understanding of the security risk assessment process will be able to more confidently scope their security risk assessments to meet their objectives in the most effective manner. Security assessment services can range from a low of about $35,000 to a high of well over $350,000, depending on various factors (see Section 2.2 for a discussion of these factors).

A more educated consumer will be better suited to solicit and review proposals presented by various security service consultancies. Security service consumers who understand the process, components, skills, required experience, and other factors of a security risk assessment will be well positioned to commission a security risk assessment that meets their needs from a quality security service provider at a competitive price.

Exercises

1. Security testing can be applied to any number or subset of controls. What controls are being tested during each of the following tests? (Be as specific as possible.)
   a. Vulnerability scanning
   b. Penetration testing
   c. Social engineering
   d. Physical penetration testing
   e. War dialing
2. Review the definition of *security risk assessment* in Section 1.4.2 and compare/contrast with another definition you or others have used.

3. List the primary benefits of a security risk assessment.
4. Find an example of a security risk assessment Request for Proposal (RFP) online. Review the required services and discuss if this is truly a security risk assessment or a related activity. How would you modify or amend the RFP to align it with the goals of a security risk assessment?
5. If security spending is not based on a security risk assessment, how are spending priorities typically determined?

Notes

1. A more complete comparison of these information security regulations is presented in Chapter 13.
2. The reader should be careful not to draw too many conclusions from such a high-level analysis of these regulations and guidelines. For example, some regulations or guidelines may not explicitly call for information security policies (as in GLBA) or configuration management (as in GAISP, HIPAA, and GLBA). However, this does not mean that those security practices should not or do not need to be part of an information security program under those regulations or guidelines. Every guideline and regulation includes security risk assessment, and therefore the inclusion of many security practices is a matter of analysis and judgment.
3. *IT Governance Institute, IT Control Objectives for Sarbanes-Oxley: The Importance of IT in the Design, Implementation, and Sustainability of Internal Control over Disclosure and Financial Reporting*, 2004.
4. Statement on Auditing Standards (SAS) No. 70, Service Organizations, was developed by the American Institute of Certified Public Accountants (AICPA, 2004) and provides a methodology for the service organization to claim internal control objectives and for the auditors to check the validity of such claims.
5. There is considerable debate as to the usefulness of SAS No. 70 and other control-objective-based audits. In these types of audits, the organization being assessed is responsible for creating its own statements of security. For example, if the organization believes that it provides effective controls over stored data, then it makes a statement regarding those controls. The debate centers around the practice of assessed organizations simply deleting or rewording any control objectives for which they cannot show reasonable assurance that those objectives are met. This practice leads security professionals to question the value of an SAS 70 audit report when it may contain few relevant control objectives. On the other side of the debate, security audit professionals are responsible for ensuring that a reasonable set of control objectives is applied to their customers. Any suggested wording or deletion of control objectives

should be approved by the auditing firm. In either case, consumers of an SAS 70 or other control-objective-based audit would be well advised to study the control objectives contained in the report and base their assurance in the report on the relevance of the control objectives for which the organization was audited.

References

American Institute of Certified Public Accountants. 2004. *Service Organizations: Applying SAS No. 70, as Amended: AICPA Guide.*

An Introduction to Computer Security: A NIST Handbook. October 1995. NIST Special Publication 800-12. http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html (accessed 8/1/03).

ASIS International. November 13, 2002. *The General Security Risk Assessment Guideline.*

International Organization for Standardization, International Electrotechnical Commission, "Information Technology—Code of Practice for Information Security Management." December 1, 2000. ISO/IEC: 27001/2, 1st ed.

Risk Management Guide: Recommendations of the National Institute of Standards and Technology. July 2002. NIST Special Publication 800-30. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (accessed 8/1/03).

Bibliography

AT&T Corp. PR Newswire, "Security Is Top Concern for Corporate Networks, According to Global Survey of Senior Executives," July 14, 2004.

CobiT Steering Committee, IT Governance Institute, *COBIT Control Objectives, 3rd ed.*, July 2000.

CobiT Steering Committee, IT Governance Institute, *COBIT Executive Summary, 3rd ed.*, July 2000.

CobiT Steering Committee, IT Governance Institute, *COBIT Framework, 3rd ed.*, July 2000.

CobiT Steering Committee, IT Governance Institute, *COBIT Management Guidelines, 3rd ed.*, July 2000.

Cosgrove, Lorraine. "CSOs Prioritize Security Spending for 2003," CSO *Online, CSO Research Reports*, January 7, 2003.

Ernst & Young. "Global Information Security Survey 2003," No. FF0224.

Federal Trade Commission. "Standards for Privacy of Individually Identifiable Health Information; Final Rule," 45 CFR Parts 160 and 164, *Federal Register, Vol.* 67, No. 157, August 14, 2002. http://www.hhs.gov/ocr/hipaa/privrulepd.pdf (accessed 8/1/03).

Federal Trade Commission. "Standards for Safeguarding Customer Information; Final Rule," 16 CFR Part 314, *Federal Register, Vol.* 67, No. 100, May 23, 2002. http://www.ftc.gov/os/2002/05/67fr36585.pdf (accessed 8/1/03).

Free Dictionary, The. www.thefreedictionary.com.

Gold Wire Technology. "Gold Wire: Survey Shows Security Still Top Concern," April 13, 2004.

Martin, James A. "Security Spending on the Rise," *iQMagazine*, September/October 2003.

United States General Accounting Office, Accounting and Information Management Division, "Information Security Risk Assessment: Practices of Leading Organizations," A Supplement to GAO's May 1998 Executive Guide on Information Security Management, GAO/IAM-00-33, November 1999.

Chapter 2

Information Security Risk Assessment Basics

It is the aim of this book to provide an extensive discussion of information security risk assessment. As such, you will find detailed information, discussion, and advice on all elements of the information security risk assessment. Many of the sections of this book will provide a rather detailed discussion of a single element of information security risk assessment. However, before we get into this level of discussion, it would be useful to provide a brief overview of the information security risk assessment process.

For the purposes of this book, the information security risk assessment process is defined as follows:

> Security Risk Assessment—An objective analysis of the effectiveness of the current security controls that protect an organization's assets and a determination of the probability of losses to those assets.

There are many security risk assessment methods available and currently in use. Depending on the specific one employed, a security risk assessment may have any number of steps or phases, and each of these phases may have slightly different names. However, the overall process is largely similar in all these methods. The generic phases of a security risk assessment are shown in Figure 2.1.

2.1 Phase 1: Project Definition

As with many projects, the success of the security risk assessment project relies not only on the skill and experience of the team assigned to the security risk assessment,

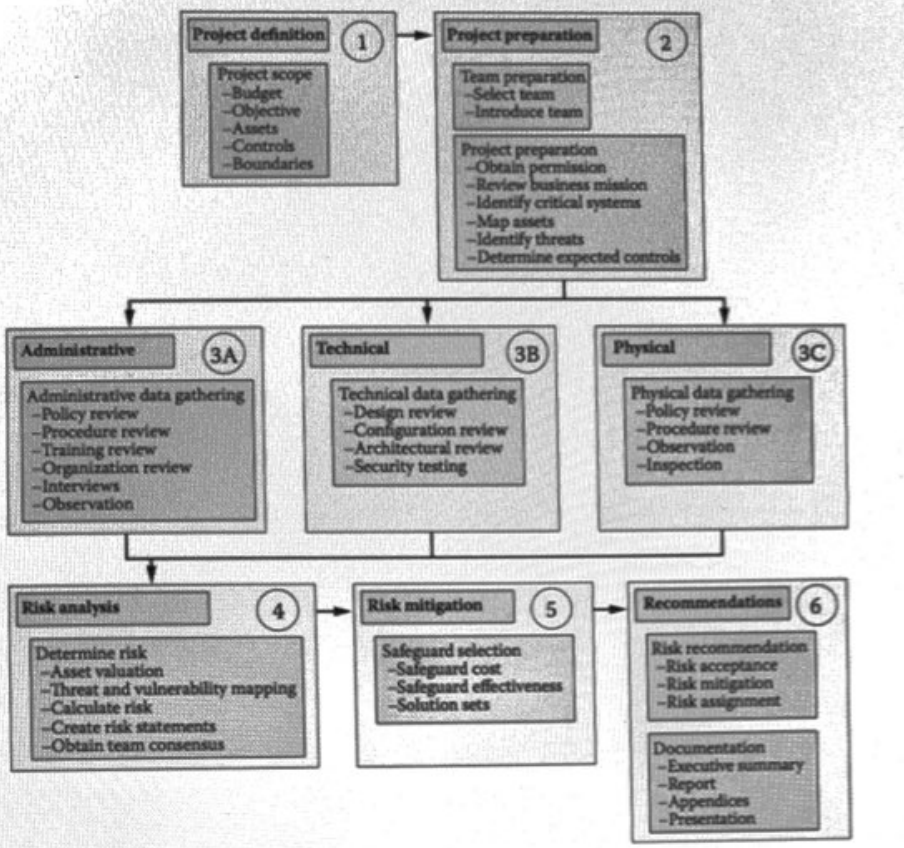

Figure 2.1 The security risk assessment process comprises the following phases: project definition, project preparation, administrative data-gathering, technical data-gathering, physical data-gathering, risk analysis, risk mitigation, and recommendations. These phases are described in more detail in the remaining chapters of this book.

but also on the effectiveness of the project management. A key component of project management is arriving at an agreement as to the scope and content of deliverables. Within the project-definition phase, the project is properly scoped and documented.

The scoping of any project includes a clear understanding of the cost and time frame of the engagement. The security risk assessment team leader needs to ensure that the project budget and time constraints are well understood. Documentation of this understanding is captured in the project plan and in the contract, if this involves a customer. A project plan not only documents the budget and time constraints, but breaks down the overall project into manageable tasks and allocates resources to those tasks.

Beyond the budget and time constraints of the project, the scoping of a security risk assessment can be more complex than the scoping of some other projects. Unique variables to the security risk assessment process include the assessment objective, the

assets and controls to be covered, and the assessment boundaries. Obtaining clarity on the security risk assessment objective is necessary to understand the customer needs. For example, a security risk assessment performed for contract compliance has a different objective than one performed for program review. The team must also seek clarity on the boundaries of the assessment through an identification of assets, systems, and other boundaries of the project. Each of these tasks is discussed in greater detail in Chapter 3.

2.2 Phase 2: Project Preparation

Based on the scope of the security risk assessment project identified in phase 1, the team leadership needs to ensure that adequate preparations are performed prior to entering the data-gathering phase. Preparation includes team preparation and project preparation.

Team preparation comprises the selection of the security risk assessment team and the introduction of the team to the organization to be assessed. Many factors go into the proper selection of the security risk assessment team, including objectivity, expertise, and experience. Introduction of the team to the customer includes formal letters of introduction as well as a request for permission and access. Each of these tasks is discussed in greater detail in Chapter 4.

2.3 Phase 3: Data Gathering

The data-gathering phase is typically performed on site and results in the collection of information concerning the effectiveness of the current administrative, physical, and technical security controls. The security risk assessment team will review the administrative controls through the collection, review, and analysis of available policies and procedures as well as observation and interviews with staff. The physical security controls will be assessed through techniques such as observation, testing, and analysis. The technical security controls will be reviewed through technical analysis, testing, and review of logs. The data-gathering phase is the most comprehensive of all of the phases and is discussed in more detail in Chapter 5. Specific advice on how to perform data-gathering for administrative, technical, and physical controls are found respectively in Chapter 6.

2.4 Phase 4: Risk Analysis

The risk-analysis phase involves a review of the data gathered and an analysis of the resulting risk to the organization. During this phase, the security risk assessment team must determine asset values, system criticality, likely threats, and the

existence of vulnerabilities based on the data gathered. Furthermore, the team must calculate the risk to the organization for each threat/vulnerability pair. The calculation and presentation of these risks can vary greatly, depending on the security risk assessment method being used.

Several elements of the risk analysis phase are considered key concepts within security risk assessments. These include assets, threats, vulnerabilities, and security risk.

2.4.1 Assets

The first element to be considered and discussed in an information security risk assessment is the assets of the organization. Assets are the items considered valuable by the organization. Later in this book, we shall discuss classes of assets, valuation of assets, and grouping of assets, but for now it is important to understand that assets are the information, resources, or other items that have value to the organization. Examples include buildings, equipments, personnel, organization reputation,[1] business documents, and many other tangible and intangible items.

Assets are an important element of a security risk assessment for several reasons. First, the enumeration of assets helps to scope the security risk assessment. Scoping of the security risk assessment will be discussed later as well, but for now, consider the following example. If an organization has commissioned a security risk assessment and has dictated that the buildings and equipment are not among the assets within the scope of the security risk assessment, then a review of the physical security controls protecting the buildings and equipment would not need to be performed. In this way, the enumeration of assets helps to scope the security risk assessment.

Second, the valuation of assets helps to determine the countermeasures employed. A countermeasure is simply a control (activity, technique, or technology) that reduces the possible loss to an organization's assets (see Table 2.1). While the selection of countermeasures can be somewhat involved, it is clear that we should not spend more on the countermeasure than the possible reduction in

Table 2.1 Asset Summary

Key Concepts	*Definition*
Asset	Resource, data, or other item of value to the organization.
Asset enumeration	A listing or grouping of assets under assessment. Asset enumeration helps to scope the information security assessment.
Asset valuation	The placement of a relative or dollar value on each asset. Asset valuation is useful in determining potential loss and countermeasure selection.

Note: Assets are those items the organization wishes to protect. The enumeration and valuing of the assets scopes and guides the security risk assessment.

the organizational loss. Later in the book, we shall discuss both asset valuation and countermeasure selection.

2.4.2 Threat Agents and Threats

The next elements to be considered and discussed in an information security risk assessment are the threats and the threat agents. A threat is an event with an undesired impact. A threat agent is the entity that may cause a threat to happen. Threats and threat agents are inextricably linked, in that it is the threat agent that causes a threat to happen. A more in-depth discussion of threats, threat classes, threat environment, and threat analysis is provided in Chapter 4 (Section 4.5). The basics of threats and threat agents are presented here as a primer on the topic. Threat agents include Mother Nature and mankind. Examples of threats include earthquakes, fires, theft, insertion of malicious code, accidental disclosure, and many others.

The main reason that threat agents and threats are important elements of the information security risk assessment is that they help to determine the scope of the vulnerabilities of the system being assessed. To begin a security risk assessment, we must understand the threats from which we plan to protect the assets. It is rather naive to believe that something undesired will never happen, and it is equally naive to believe that you can possibly anticipate or even list every possible threat. However, we can describe the threat environment of the target system. This approach helps the security risk assessment team to consider those threats that are most likely to impact the target of the security risk assessment and to ignore those that are least likely to impact the target of the security risk assessment. Those threats that are considered relevant for a specific security risk assessment are called "valid threats".

For example, an information security risk assessment being performed on an organization in Austin, Texas, would not need to consider the threat of earthquakes, snow blizzards, or perhaps even hurricanes. However, it would need to consider flooding, tornadoes, and severe thunderstorms. In this example, the threat agent is Mother Nature, and we consider some of her threats valid and others not valid for this portion of the country.

2.4.2.1 Threat Agents

Threat agents are the catalyst of the threat. A threat agent is the entity that causes a threat to happen. A list of possible threat agents is provided below for illustrative purposes:

- Nature—Any number of natural disasters could affect the support systems relied upon by your organization's information system. If the threat is a natural threat, such as storms or floods, then "nature" can be considered the threat agent.
- Employees—Organizations entrust their personnel to perform their duties accurately and consistent with the policies of the organization. A major threat to organizations is the threat that an employee could make a critical mistake in data entry, release proprietary data, or decide to defraud the organization.

- Malicious Hackers—Information systems that are networked with other systems or even the Internet expose themselves to millions of potential hackers. Even those systems that do not provide a public interface, such as the Internet, are still exposed to hackers through social engineering, modem connections, or physical attacks.
- Industrial Spies—The value of proprietary information to the competition should not be underestimated. Industrial espionage is a significant threat to most organizations and can result in loss of profits, competitive advantage, or even the business itself.
- Foreign Government Spies—Foreign spies could perform espionage for the purpose of advancing the capabilities of a foreign government or restricting our government's abilities, or this area could even include foreign-sponsored industrial espionage.

2.4.2.2 *Threats*

A threat is an undesired event that may result in the loss, disclosure, or damage to an organizational asset (see Table 2.2). A partial list of threats is given below:

- Errors and Omissions—Occasionally, mistakes by authorized employees, users, developers, and testers can occur during data entry or operations, or in system or application development. These errors and omissions can lead to a lack of data and system integrity, a lack of system stability, and even disclosure of sensitive information.
- Fraud and Theft—The threat to the information system could be for the purpose of fraud or theft. Information systems are targets of fraud and theft because they directly or indirectly protect assets of value. For example, financial systems directly protect the assignment of funds to accounts, whereas inventory systems indirectly

Table 2.2 Threat and Threat Agent Summary

Key Concepts	*Definition*
Threat	
Valid threat	Threats that are considered relevant for a specific security risk a assessment
Threat agent	The entity that may cause a threat to happen
Threat environment	Determining the physical, geographical, and other aspects of the organization's system helps to determine the scope and extent of applicable threats

Note: Threats and threat agents are the actions and entities the organization would like to avoid. Threats and threat agents are determined by the physical geography and mission of the organization.

protect equipment through inventory tracking. Each of these types of systems can be the target of those attempting to steal from or defraud a corporation.

- Sabotage—Those authorized by the organization to access the organization's information systems and assets must be trusted to uphold the trust placed in them. However, sometimes this trust is misplaced. Such misplaced trust leads to sabotage. Sabotage may include physical damage to facilities or equipment, destruction of processes, deletion of data, or loss of data integrity.
- Loss of Physical and Infrastructure Support—The physical and infrastructure support provides the required services for an organization's information systems, such as power, communication, and transportation. Many threats, both natural and human, endanger the ability of the support structure to supply the required services to the information system. Threats in this category include power failures, winter storms, labor strikes, and terrorist attacks.
- Espionage—Proprietary information is a highly valued asset of the organization. Proprietary information is also highly valued by the competition. The act of gathering proprietary data for the purpose of aiding another organization is referred to as "espionage." Espionage is performed by foreign governments and competitive organizations.
- Malicious Code—The connectivity of systems and the introduction of new software and data from other sources increases the threat that an organization's information system may become infected with malicious software. Malicious software could be a virus, Trojan horse, worm, logic bomb, or other software that does not perform as intended.
- Disclosure—Information systems contain vast amounts of data that are sensitive to the organization and to individuals. The concern that data about an individual could be disclosed to someone unauthorized is referred to as "privacy." The concern that data about the organization could be disclosed is referred to as "confidentiality." Both the personal privacy threat and the organizational confidentiality threat are major concerns.

2.4.3 Vulnerabilities

A vulnerability is a flaw or oversight in an existing control that may possibly allow a threat agent to exploit it to gain unauthorized access to organizational assets. In Chapters 6, 7, and 8 we shall discuss in detail how to find and describe vulnerabilities in administrative, technical and physical controls. In Chapter 9, we shall discuss how to rate these vulnerabilities. For now, it is important to understand the relationship of vulnerabilities to other elements of the information security risk assessment and the importance of the vulnerability in this effort.

Vulnerabilities are important elements of a security risk assessment because they are instrumental in determining existing and residual risk. Without vulnerabilities, there would be no risk. However, we know there is no such thing as a system without vulnerabilities, so it is the task of the security risk assessment team to assess the vulnerabilities in

the existing system and those vulnerabilities that are likely to still exist if the safeguard recommendations are implemented. When assessing vulnerabilities in the system, it is useful to categorize the vulnerabilities according to administrative, physical, and technical areas, since the departments or personnel are likely to be distributed similarly.

Administrative vulnerabilities are those vulnerabilities that exist in policies, procedures, or security activities. Examples include missing acceptable-use policies, gaps in termination procedures, or the lack of independence in security testing.[2] Physical vulnerabilities are those vulnerabilities that exist in the physical, geographical, personnel, or utility provisioning controls. Examples include holes in the fence line, location in a flight path, lack of background checks for sensitive positions, and lack of redundant power supplies. Technical vulnerabilities are those that exist in the logical controls in the organization's system. Examples include misconfigured routers, backdoors in programs, and weak passwords (see Table 2.3).

2.4.4 Security Risk

A security risk is the loss potential to an organization's asset(s) that will likely occur if a threat is able to exploit a vulnerability. In this book, we shall discuss various ways to assess (Chapter 9), reduce (Chapter 10), and report security risk (Chapter 11). Security risk (and residual security risk) is the key element of the information security risk assessment because it is the culmination of all the other assessments, calculations, and analyses. Security risk is the key measurement that

Table 2.3 Vulnerability Summary

Key Concepts	*Definition*
Vulnerability	A flaw or oversight in an existing control that may allow a threat agent to exploit it to gain unauthorized access to organizational assets
Administrative vulnerability	Gaps in policies, procedures, or security activities, e.g., missing acceptable-use policies, gaps in termination procedures, or the lack of independence in security testing
Physical vulnerability	Gaps in physical, geographical, personnel, or utility provisioning controls, e.g., holes in the fence line, location in a flight path, lack of background checks for sensitive positions, and lack of redundant power supplies
Technical vulnerability	Gaps in the logical controls in the organization's system, e.g., misconfigured routers, back doors in programs, and weak passwords

Note: Vulnerabilities are weaknesses or absences of security control. These vulnerabilities can exist in administrative, physical, or technical controls.

the organization's management really cares about; the rest of the stuff is just a way to get to the key measurement of security risk.

There are many key factors to consider when discussing security risk, but the most important factor of security risk to consider right now is the manner in which the security risk is derived and presented. There are many ways to derive and present security risk, but all of these approaches can be described as quantitative or qualitative.

The quantitative approach to deriving and presenting security risk relies on specific formulas and calculations to determine the value of the security risk. A quantitative approach to determining and even presenting security risk has the advantages of being objective and expressed in terms of dollar figures. However, such quantitative calculations can be rather complex, and accurate values for the variables in quantitative formulas may be difficult to obtain.

The qualitative approach to deriving and presenting security risk relies on subjective measures of asset valuation, threats, vulnerabilities, and ultimately the security risk. A qualitative approach to determining and presenting security risk has the advantage of being easy to understand and, in many cases, provides adequate indication of the organization's security risk. However, a security risk measurement derived from such qualitative measures is, indeed, subjective and may not be trusted by some in management positions (see Table 2.4). More detail on security risk analysis is provided in Chapter 9.

2.5 Phase 5: Risk Mitigation

Based on the risks defined in the risk analysis phase, the team must develop recommendations for safeguards to reduce the identified risks to an acceptable level. The safeguard selection process involves mapping safeguards to threat/vulnerability pairs, determining the reduction of risk, determining the cost of the safeguard, and grouping safeguards into solution sets.

Several elements of the risk mitigation phase are considered key concepts within security risk assessments. These include safeguards and residual risk.

2.5.1 Safeguards

Next we consider the security controls, or safeguards, put in place to protect the organization's assets from reasonable threats. A safeguard or countermeasure is a technique, activity, or technology employed to reduce the risk to the organization's assets. A safeguard may prevent, detect, or minimize the potential loss to an organization's assets. For this reason, safeguards are generally categorized as preventive, detective, or corrective measures. Preventive measures are controls that are designed to deter undesirable events from happening. Examples include access controls, door locks, and security awareness training. Detective measures are controls that identify conditions that indicate that an undesirable event has

Table 2.4 Security Risk Summary

Key Concepts	*Definition*	
Security risk		
Quantitative risk	A method of determining and presenting security risk that relies on specific formulas and calculations to determine the value of the security risk	
	Advantages	Disadvantages
	Objective; security risk expressed in terms of dollars	Security risk calculations are complex; accurate values are difficult to obtain
Qualitative risk	A method of determining and presenting security risk that relies on subjective measures of asset valuation, threats, vulnerabilities, and ultimately of the security risk	
	Advantages	Disadvantages
	Easy to understand; provides adequate indication of the organization's security risk	Subjective; may not be trusted by some in management positions

Note: Security risks are a measurement of the likelihood that the organization's assets are susceptible. Security risk assessment methods can be either quantitative or qualitative.

happened. Examples of detective measures include audit logs, security testing, and intrusion detection systems. Corrective measures are controls designed to correct the damage caused by undesirable events. Examples of corrective measures include security guards, termination policies, and file recovery. Note that safeguards (also referred to as controls) may be classified as being in multiple categories, such as security guards, which can be considered a preventive, detective, and corrective measure.

Safeguards are an important element in information security risk assessments for two reasons. First, all existing safeguards must be considered when determining the present vulnerability of the organization's system. If the security risk assessment team fails to consider all the safeguards in place to protect the organization's assets, then the security risk assessment results will be inaccurate and will likely err on the side of overestimating the risk. Such errors can be costly, as decisions for implementing additional security measures should be based on the results of security risk assessments.

Second, safeguards are an important element of security risk assessments because the final report should recommend safeguards to be implemented to bring the residual risk within tolerance levels of the senior management of the

Table 2.5 Safeguard Summary

Definition: A technique, activity, or technology employed to reduce the risk to the organization's assets. Safeguards protect the organization's assets from the risks of threats.	
Key concepts	
Preventive	Controls designed to deter undesirable events from happening, e.g., access controls, door locks, and security awareness training
Detective	Controls that identify conditions that indicate that an undesirable event has happened, e.g., audit logs, security testing, and intrusion detection systems
Corrective	Controls designed to correct the damage caused by undesirable events, e.g., security guards, termination policies, and file recovery

organization. Safeguard recommendations are key to the results of a security risk assessment and must be carefully considered (see Table 2.5).

2.5.2 Residual Security Risk

Residual security risk is the security risk that remains after implementation of recommended safeguards. The objective of security risk management is to accurately measure the residual security risk and keep it to a level at or below the security risk tolerance level.

Residual security risk is an important element of information security risk assessments for several reasons. First and foremost, residual risk is the security risk that the organization will inherit when safeguards are implemented. It is important that the organization's management fully understands the concept of residual security risk and is comfortable with staffing and budgeting decisions that determine the residual security risk level.

Second, the security professional and the organization's management must clearly understand that there is no such thing as 100 percent security (or 0 percent residual security risk). Even if the organization implements every one of the information security professionals' recommendations, the organization still has some residual security risk to its assets. More detail about security risk mitigation is provided in Chapter 10. Table 2.6 provides a definition of residual security risk as well as some key concepts.

2.6 Phase 6: Risk Reporting and Resolution

The final phase of a security risk assessment is the risk reporting and resolution phase. During this phase, the security risk assessment team develops a report and

Table 2.6 Residual Risk Summary

Definition: The security risk that remains after implementation of recommended safeguards. Residual risks are the leftover risks to the organization's assets after safeguards have been applied.	
Key concepts	
Static risk	The security risk that will always exist
Dynamic risk	Security risk that may be reduced through the implementation of safeguards

a presentation to the project sponsor that clearly identifies the risks found and the safeguards recommended. The final risk assessment report should provide clear information for the executive, management, and technical personnel. The executives of the assessed organization must then determine the resolution of the identified risks. The risk resolution element within this phase is considered a key concept within security risk assessments.

2.6.1 Risk Resolution

At the conclusion of a security risk assessment project, the senior management of the assessed organization must determine the resolution of each of the identified risks. In other words, the senior manager must decide to reduce the risk, accept the risk, or delegate the risk to someone else.[3]

A security risk can be reduced by implementing additional security controls or even by improving existing security controls. Suggestions for risk-reducing safeguards for each identified risk should be documented in the final report. Along with these recommendations, cost and effectiveness estimations should be included to assist in the senior manager's decision.

A security risk can be accepted if the senior manager believes that it is in the best interest of the organization to accept the risk rather than to accept the cost burdens of implementing additional safeguards. The acceptance of this risk must be performed by a senior manager of the organization, because this decision impacts the organization as a whole and not just a single department or project.

Lastly, a security risk can be transferred to another organization such as an outsourcing company or an insurance agency. The transfer of security risk is a contractual agreement that clearly spells out the risk and the burden accepted along with the conditions and limitations of such an agreement (see Table 2.7). More detail on security risk assessment reporting in provided in Chapter 11.

Table 2.7 Risk Resolution Summary

Key Concepts	*Definition*
Risk resolution	The decision by senior management of how to resolve the risk presented to them
Risk reduction	The reduction of risk to the organization to an acceptable level through the adoption of additional security controls or improvement of existing controls
Risk acceptance	The deliberate decision by senior management to accept an identified risk based on the business objectives of the organization
Risk transference	The contractual transfer of risk to another organization through outsourcing or insurance

Note: Safeguards protect the organization's assets from the risks of threats.

Exercises

1. Tasks performed within a security risk assessment have some flexibility in terms of order performed (consider Figure 2.1). Indicate the order of the tasks below by listing prerequisite tasks (tasks that must be completed prior to starting) and successors (tasks that cannot begin prior to completion of current task) for each of the tasks listed below:

Be Prepared to Justify Your Answers

Prerequisite Tasks	*Task*	*Successor Tasks*
	a. Project scope	
	b. Asset valuation	
	c. Threat identification	
	d. Policy review	
	e. Vulnerability scan	
	f. Schedule interviews	
	g. Perform interviews	
	h. Assess risk	
	i. Develop recommendations	
	j. Present report	

3. Another valid management action for an identified risk is to obtain additional data. This would be especially valid in cases where a security risk assessment was performed with little rigor (e.g., survey-based) and the potential mitigation strategies are expensive. Additional data supplied by a more rigorous review (e.g., interviews, observations, and testing) can give management a more appropriate amount of information for decisions involving large expenditures.

References

Common Criteria for Information Technology Security Evaluation. Version 3.1, Revision 3 Final CCIMB-2009-07-001, July 2009.

Tipton, Harold F. and Micki Krause. *Information Security Management Handbook*, 2007.