CHAPTER 16

IT Security Management and Risk Assessment

16.1 **IT Security Management**

16.2 **Organizational Context and Security Policy**

16.3 **Security Risk Assessment**

Baseline Approach
Informal Approach
Detailed Risk Analysis
Combined Approach

16.4 **Detailed Security Risk Analysis**

Context and System Characterization
Identification of Threats/Risks/Vulnerabilities
Analyze Risks
Evaluate Risks
Risk Treatment

16.5 **Case Study: Silver Star Mines**

16.6 **Recommended Reading and Web Sites**

16.7 **Key Terms, Review Questions, and Problems**

In previous chapters, we discussed a range of technical and administrative measures that can be used to manage and improve the security of computer systems and networks. In this chapter and the next, we look at the process of how to best select and implement these measures to effectively address an organization's security requirements. As we noted in Chapter 1, this involves examining three fundamental questions:

1. What assets do we need to protect?
2. How are those assets threatened?
3. What can we do to counter those threats?

IT security management is the formal process of answering these questions, ensuring that critical assets are sufficiently protected in a cost-effective manner. More specifically, IT security management consists of first determining a clear view of an organization's IT security objectives and general risk profile. Next an IT security risk assessment is needed for each asset in the organization that requires protection; this assessment must answer the three key questions listed above. This assessment provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified to an acceptable level, eliminate them, or provide mitigating controls. This chapter will consider each of these items. The process continues by selecting suitable controls and then writing plans and procedures to ensure that these necessary controls are implemented effectively. That implementation must be monitored to determine if the security objectives are met. The whole process must be iterated, and the plans and procedures kept up-to-date, because of the rapid rate of change in both the technology and the risk environment. We discuss the latter part of this process in Chapter 17.

16.1 IT SECURITY MANAGEMENT

The discipline of IT security management has evolved considerably over the last few decades. This has occurred in response to the rapid growth of, and dependence on, networked computer systems and the associated rise in risks to these systems. In the last decade a number of national and international standards have been published. These represent a consensus on the *best practice* in the field. The International Standards Organization (ISO) is currently revising and consolidating a number of these standards into the ISO 27000 series. Table 16.1 details a number of existing and proposed standards associated with this family. In the United States, NIST has produced a number of relevant standards, including [NIST02], [NIST05], and [NIST06]. With the growth of concerns about corporate governance following events such as the Enron collapse and repeated incidences of the loss of personal information by government organizations, auditors for such organizations increasingly request adherence to formal standards such as these.

Table 16.1 ISO 27000 Series and Related Standards

ISO27000	A proposed standard that will define the vocabulary and definitions used in the 27000 family of standards.
ISO27001	Defines the information security management system specification and requirements against which organizations are formally certified. It replaces the older Australian and British national standards AS7799.2 and BS7799.2.
ISO27002 (ISO17799)	Currently published and better known as ISO17799, this standard specifies a code of practice detailing a comprehensive set of information security control objectives and a menu of best practice security controls. It replaces the older Australian and British national standards AS7799.1 and BS7799.1.
ISO27003	A proposed standard containing implementation guidance on the use of the 27000 series of standards following the "Plan-Do-Check-Act" process quality cycle. Publication is proposed for late 2008.
ISO27004	A draft standard on information security management measurement to help organizations measure and report the effectiveness of their information security management systems. It will address both the security management processes and controls. Publication is proposed for 2007.
ISO27005	A proposed standard on information security risk management. It will replace the recently released British national standard BS7799.3. Publication is proposed for 2008/2009.
ISO13335	Provides guidance on the management of IT security. This standard comprises a number of parts. Part 1 defines concepts and models for information and communications technology security management. Part 2, currently in draft, will provide operational guidance on ICT security. These replace the older series of 5 technical reports ISO/IEC TR 13335 parts 1–5.

[ISO13335] provides a conceptual framework for managing security. It defines **IT Security Management** as follows:

IT SECURITY MANAGEMENT: A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability. IT security management functions include:

- determining organizational IT security objectives, strategies, and policies
- determining organizational IT security requirements
- identifying and analyzing security threats to IT assets within the organization
- identifying and analyzing risks
- specifying appropriate safeguards
- monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization
- developing and implementing a security awareness program
- detecting and reacting to incidents

This process is illustrated in Figure 16.1 (adapted from figures 8, 9, and 12 in [ISO13335]), with a particular focus on the internal details relating to the risk assessment process. It is important to emphasize that IT security management needs to be a key part of an organization's overall management plan. Similarly, the IT security risk assessment process should be incorporated into the wider risk assessment of all the organization's assets and business processes. Hence, unless senior management in an organization are aware of, and support, this process, it is unlikely that the desired security objectives will be met and contribute appropriately to the organization's business outcomes. Note also that IT management is not something undertaken just once. Rather it is a cyclic process that must be repeated constantly in order to keep pace with the rapid changes both in IT technology and the risk environment.

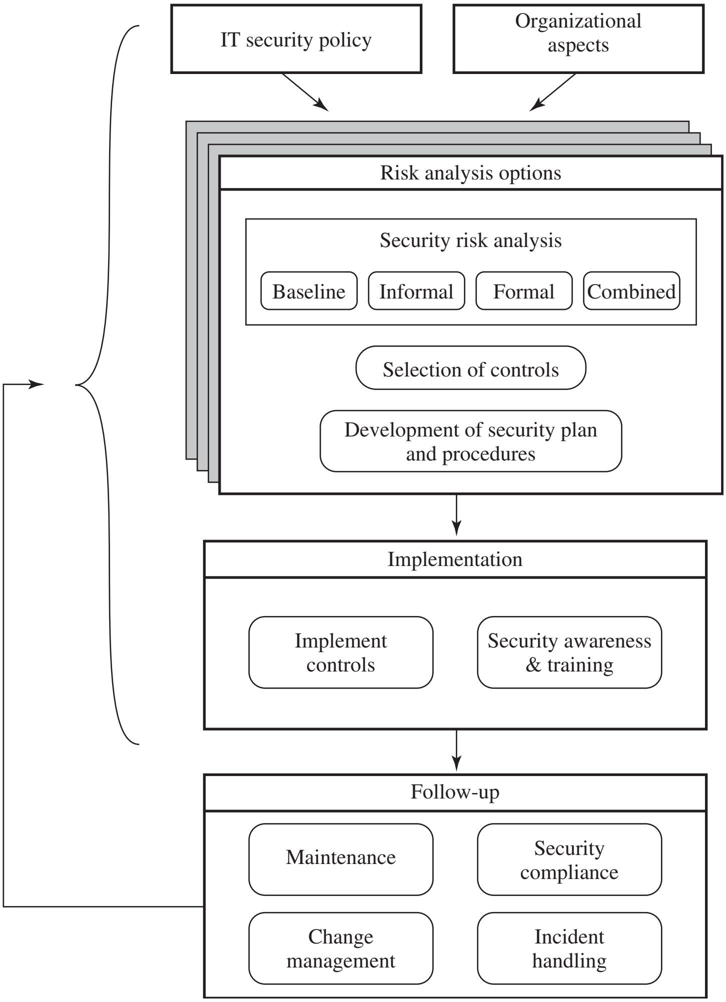

Figure 16.1 **Overview of IT Security Management**

The iterative nature of this process is a key focus of [ISO27001]. This standard details a model process for managing information security that comprises the following steps[1]:

Plan establish security policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

Do implement and operate the security policy, controls, processes and procedures.

Check assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.

Act take corrective and preventive actions, based on the results of the internal security audit and management review or other relevant information, to achieve continual improvement of the security management process.

This process is illustrated in Figure 16.2 (adapted from figure 1 in [ISO27001]). Compare this figure with Figure 16.1. The development of the organization's IT security objectives, strategies, and policies; the risk assessment; and the development of an IT security plan all clearly constitute the *plan* stage of this process. The implementation aspects constitute the *do* stage. The follow-up forms the *check* stage. Lastly, the feedback of details from the follow-up aspects to all earlier stages in the process comprises the *act* stage of this model. The outcome of this process should be that the security needs of the interested parties are managed appropriately.

16.2 ORGANIZATIONAL CONTEXT AND SECURITY POLICY

The initial step in the IT security management process comprises an examination of the organization's IT security objectives, strategies, and policies, in the context of the organization's general risk profile. This can only occur in the context of the wider organizational objectives and policies, as part of the management of the organization. Organizational security objectives identify what IT security outcomes should be achieved. They need to address individual rights, legal requirements, and standards imposed on the organization, in support of the overall organizational objectives. Organizational security strategies identify how these objectives can be met. Organizational security policies identify what needs to be done. These objectives, strategies, and policies need to be maintained and regularly updated based on the results of periodic security reviews, to reflect the constantly changing technological and risk environments.

To help identify these organizational security objectives, the role and importance of the IT systems in the organization is examined. The value of these systems in assisting the organization achieve its goals is reviewed, not just the direct costs of these systems. Questions that help clarify these issues include the following:

[1] Quoted from the introduction in [ISO27001].

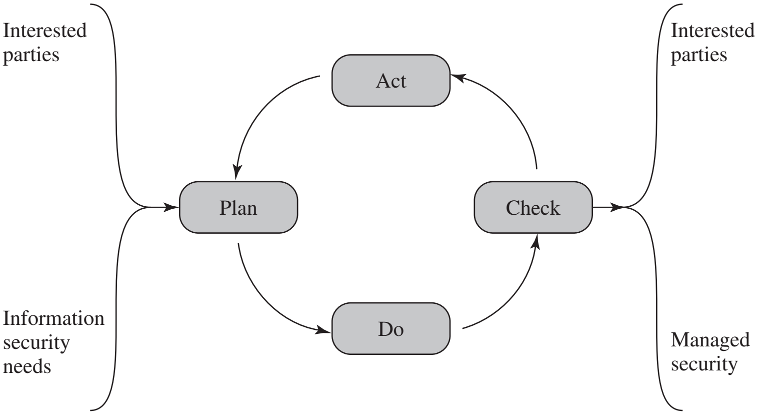

Figure 16.2 **The Plan-Do-Check-Act Process Model**

- What key aspects of the organization require IT support in order to function efficiently?
- What tasks can only be performed with IT support?
- Which essential decisions depend on the accuracy, currency, integrity, or availability of data managed by the IT systems?
- What data created, managed, processed, and stored by the IT systems need protection?
- What are the consequences to the organization of a security failure in the organization's IT systems?

If the answers to some of the above questions show that IT systems are important to the organization achieving its goals, then clearly the risks to them should be assessed and appropriate action taken to address any deficiencies identified. A list of key organization security objectives should result from this examination.

Once the objectives are listed, some broad strategy statements can be developed. These outline in general terms how the identified objectives will be met in a consistent manner across the organization. The topics and details in the strategy statements depend on the identified objectives, the size of the organization, and the importance of the IT systems to the organization. The strategy statements should address the approaches the organization will use to manage the security of its IT systems.

Given the organizational security objectives and strategies, an organizational security policy is developed that describes what the objectives and strategies are and the process used to achieve them. The organizational or corporate security policy may be either a single large document or, more commonly, a set of related documents. This policy typically needs to address at least the following topics[2]:

- The scope and purpose of the policy
- The relationship of the security objectives to the organization's legal and regulatory obligations, and its business objectives

[2] Adapted from the details provided in various sections of [ISO13335].

- IT security requirements in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability, particularly with regard to the views of the asset owners
- The assignment of responsibilities relating to the management of IT security and the organizational infrastructure
- The risk management approach adopted by the organization
- How security awareness and training is to be handled
- General personnel issues, especially for those in positions of trust
- Any legal sanctions that may be imposed on staff, and the conditions under which such penalties apply
- Integration of security into systems development and procurement
- Definition of the information classification scheme used across the organization
- Contingency and business continuity planning
- Incident detection and handling processes
- How and when this policy should be reviewed
- The method for controlling changes to this policy

The intent of the policy is to provide a clear overview of how an organization's IT infrastructure supports its overall business objectives in general, and more specifically what security requirements must provided in order to do this most effectively. It is critical that the IT security policy has full approval and buy-in by senior management. Without this, experience shows that it is unlikely that sufficient resources or emphasis will be given to meeting the identified objectives and achieving a suitable security outcome. With the clear, visible support of senior management, it is much more likely that security will be taken seriously by all levels of personnel in the organization. This support is also evidence of concern and due diligence in the management of the organization's systems and the monitoring of its risk profile.

Because the responsibility for IT security is shared across the organization, there is a risk of inconsistent implementation of security and a loss of central monitoring and control. The various standards strongly recommend that overall responsibility for the organization's IT security be assigned to a single person, the organizational IT security officer. This person should ideally have a background in IT security. The responsibilities of this person include

- Oversight of the IT security management process
- Liaison with senior management on IT security issues
- Maintenance of the organization's IT security objectives, strategies, and policy
- Coordination of the response to any IT security incidents
- Management of the organization-wide IT security awareness and training programs
- Interaction with IT project security officers

Larger organizations will need separate IT project security officers associated with major projects and systems. Their role is to develop and maintain security policies for their systems, develop and implement security plans relating to these systems, handle the day-to-day monitoring of the implementation of these plans, and assist with the investigation of incidents involving their systems.

16.3 SECURITY RISK ASSESSMENT

We now turn to the key risk management component of the IT security process. This stage is critical, because without it there is a significant chance that resources will not be deployed where most effective. The result will be that some risks are not addressed, leaving the organization vulnerable, while other safeguards may be deployed without sufficient justification, wasting time and money. Ideally every single organizational asset is examined, and every conceivable risk to it evaluated. If a risk is judged to be too great, then appropriate remedial controls are deployed to reduce the risk to an acceptable level. In practice this is clearly impossible. The time and effort required, even for large, well-resourced, organizations, is clearly neither achievable nor cost effective. Even if possible, the rapid rate of change in both IT technologies and the wider threat environment means that any such assessment would be obsolete as soon as it is completed, if not earlier! Clearly some form of compromise evaluation is needed.

Another issue is the decision as to what constitutes an appropriate level of risk to accept. In an ideal world the goal would be to eliminate all risks completely. Again, this is simply not possible. A more realistic alternative is to expend an amount of resources in reducing risks proportional to the potential costs to the organization should that risk occur. This process also must take into consideration the likelihood of the risk's occurrence. Specifying the acceptable level of risk is simply prudent management and means that resources expended are reasonable in the context of the organization's available budget, time, and personnel resources. The aim of the risk assessment process is to provide management with the information necessary for them to make reasonable decisions on where available resources will be deployed.

Given the very wide range of organizations, from very small businesses to global multinationals and national governments, there clearly needs to be a range of alternatives available in performing this process. There are a range of formal standards that detail suitable IT security risk assessment processes, including [ISO13335] and [NIST02]. In particular, [ISO13335] recognizes four approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline approach
- Informal approach
- Detailed risk analysis
- Combined approach

The choice among these will be determined by the resources available to the organization and from an initial high-level risk analysis that considers how valuable the IT systems are and how critical to the organization's business objectives. Legal and regulatory constraints may also require specific approaches. This information should be determined when developing the organization's IT security objectives, strategies, and policies.

Baseline Approach

The baseline approach to risk assessment aims to implement a basic general level of security controls on systems using baseline documents, codes of practice, and *industry best practice*. The advantages of this approach are that it doesn't require the expenditure of additional resources in conducting a more formal risk assessment and that the same measures can be replicated over a range of systems. The major disadvantage is that no special consideration is given to variations in the organization's risk exposure based on who they are and how their systems are used. As well, there is a chance that the baseline level may be set either too high, leading to expensive or restrictive security measures that may not be warranted, or too low, resulting in insufficient security and leaving the organization vulnerable.

The goal of the baseline approach is to implement generally agreed safeguards to provide protection against the most common threats. These would include implementing industry best practice in configuring and deploying systems, like those we discuss in Chapters 23 and 24 for Linux and Windows security. As such, the baseline approach forms a good base from which further security measures can be determined. Suitable baseline recommendations and checklists documents may be obtained from a range of organizations, including

- Various national and international standards organizations
- Security-related organizations such as the CERT, NSA, and so on
- Industry sector councils or peak groups

The use of the baseline approach alone would generally only be recommended for small organizations without the resources to implement more structured approaches. But it will at least ensure that a basic level of security is deployed, which is not guaranteed by the default configurations of many systems.

Informal Approach

The informal approach involves conducting some form of informal, pragmatic risk analysis for the organization's IT systems. This analysis does not involve the use of a formal, structured process, but rather exploits the knowledge and expertise of the individuals performing this analysis. These may either be internal experts, if available, or, alternatively, external consultants. A major advantage of this approach is that the individuals performing the analysis require no additional skills. Hence an informal risk assessment can be performed relatively quickly and cheaply. In addition, because the organization's systems are being examined, judgments can be made about specific vulnerabilities and risks to systems for the organization that the baseline approach would not address. Thus more accurate and targeted controls may be used than would be the case with the baseline approach. There are a number of disadvantages. Because a formal process is not used, there is a chance that some risks may not be considered appropriately, potentially leaving the organization vulnerable. As well, because the approach is informal, the results may be skewed by the views and prejudices of the individuals performing the analysis. The approach may also result in insufficient justification for suggested controls, leading to questions over whether the proposed expenditure is really justified. Lastly, there may be inconsistent results over time as a result of differing expertise in those conducting the analysis.

The use of the informal approach would generally be recommended for small to medium-sized organizations where the IT systems are not necessarily essential to meeting the organization's business objectives and where additional expenditure on risk analysis cannot be justified.

Detailed Risk Analysis

The third and most comprehensive approach is to conduct a detailed risk assessment of the organization's IT systems, using a formal structured process. This provides the greatest degree of assurance that all significant risks are identified and their implications considered. This process involves a number of stages, including identification of assets, identification of threats and vulnerabilities to those assets, determination of the likelihood of the risk occurring and the consequences to the organization should that occur, and hence the risk the organization is exposed to. With that information, appropriate controls can be chosen and implemented to address the risks identified. The advantages of this approach are that it provides the most detailed examination of the security risks of an organization's IT system and produces strong justification for expenditure on the controls proposed. It also provides the best information for continuing to manage the security of these systems as they evolve and change. The major disadvantage is the significant cost in time, resources, and expertise needed to perform such an analysis. The time taken to perform this analysis may also result in delays in providing suitable levels of protection for some systems. The details of this approach are discussed in the next section.

The use of a formal, detailed risk analysis is often a legal requirement for some government organizations and businesses providing key services to them. This may also be the case for organizations providing key national infrastructure. For such organizations, there is no choice but to use this approach. It may also be the approach of choice for large organizations with IT systems critical to their business objectives and with the resources available to perform this type of analysis.

Combined Approach

The last approach combines elements of the baseline, informal, and detailed risk analysis approaches. The aim is to provide reasonable levels of protection as quickly as possible, and to then to examine and adjust the protection controls deployed on key systems over time. The approach starts with the implementation of suitable baseline security recommendations on all systems. Next, systems either exposed to high-risk levels or critical the organization's business objectives are identified in the high-level risk assessment. A decision can then be made to possibly conduct an immediate informal risk assessment on key systems, with the aim of relatively quickly tailoring controls to more accurately reflect their requirements. Lastly, an ordered process of performing detailed risk analyses of these systems can be instituted. Over time this can result in the most appropriate and cost-effective security controls being selected and implemented on these systems. This approach has a significant number of advantages. The use of the initial high-level analysis to determine where further resources need to be expended, rather than facing a full detailed risk analysis of all systems, may well be easier to sell to management. It also results in the development of a strategic picture of the IT resources and where major risks are likely to occur. This provides a key planning aid in the subsequent management of the organization's security. The use of the baseline and informal analyses ensures that a basic level of security protection is implemented early. And it means that resources are likely to be applied where most needed and that systems most at risk are likely to be examined further reasonably early in the process. However, there are some disadvantages. If the initial high-level analysis is inaccurate, then some systems for which a detailed risk analysis should be performed may remain vulnerable for some time. Nonetheless, the use of the baseline approach should ensure a basic minimum security level on such systems. Further, if the results of the high-level analysis are reviewed appropriately, the chance of lingering vulnerability is minimized.

[ISO13335] considers that for most organizations, in most circumstances, this approach is the most cost effective. Consequently its use is highly recommended.

16.4 DETAILED SECURITY RISK ANALYSIS

The formal, detailed security risk analysis approach provides the most accurate evaluation of an organization's IT system's security risks, but at the highest cost. This approach has evolved with the development of trusted computer systems, initially focused on addressing defense security concerns, as we discuss in chapter 10. The original security risk assessment methodology was given in the Yellow Book standard (CSC-STD-004-85 June 1985), one of the original U.S. TCSEC rainbow book series of standards. Its focus was entirely on protecting the confidentiality of information, reflecting the military concern with information classification. The recommended rating it gave for a trusted computer system depended on difference between the minimum user clearance and the maximum information classification. Specifically it specified a risk index as

$$\text{Risk Index} = \text{Max Info Sensitivity} - \text{Min User Clearance}$$

A table in this standard, listing suitable categories of systems for each risk level, was used to select the system type. Clearly this limited approach neither adequately reflects the range of security services required nor the wide range of possible threats. Over the years since, the process of conducting a security risk assessment that does consider these issues has evolved.

A number of national and international standards document the expected formal risk analysis approach. These include [ISO13335], [ADSD06], [SASN04], [SA04], and [NIST02]. Its use is often mandated by government organizations and associated businesses. These standards all broadly agree on the process used. Figure 16.3 (reproduced from Fig 3-1 in [NIST02]) illustrates a typical process used.

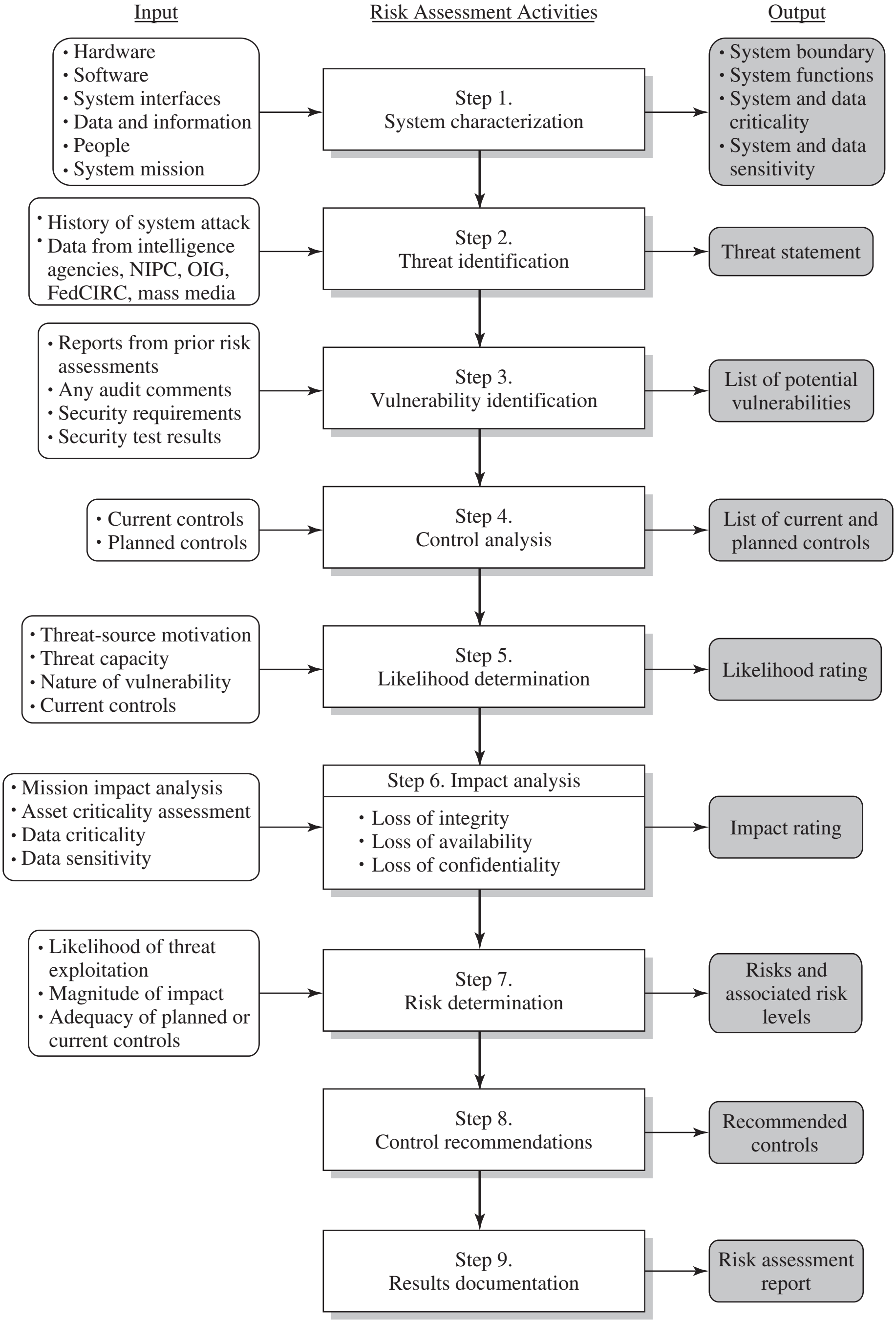

Figure 16.3 Risk Assessment Methodology

Context and System Characterization

The initial step is known as *Establishing the Context* or *System Characterization*. Its purpose is to determine the basic parameters within which the risk assessment will be conducted, and then to identify the assets to be examined.

Establishing the Context The process starts with the organizational security objectives and considers the broad risk exposure of the organization. This recognizes that not all organizations are equally at risk, but that some, because of their function, may be specifically targeted. It explores the relationship between a specific organization and the wider political and social environment in which it operates. Figure 16.4 (adapted from an IDC 2000 report) suggests a possible spectrum of organizational risk. Industries such as agriculture and education are considered to be at lesser risk compared to government or banking and finance. Note that this classification predates September 11, and it is likely that there has been change since it was developed. In particular it is likely that utilities, for example, are probably at higher risk than the classification suggests. NIST have indicated[3] that the following industries are vulnerable to risks in Supervisory Control and Data Acquisition (SCADA) and process control systems: electric, water, oil and gas (pipelines, too), chemical, pharmaceutical, pulp and paper, food and beverage, discrete manufacturing (automotive, aerospace, and durable goods), air and rail transportation, and mining and metallurgy industries.

At this point in determining an organization's broad risk exposure, any relevant legal and regulatory constraints must also be identified. These features provide a baseline for the organization's risk exposure and an initial indication of the broad scale of resources it needs to expend to manage this risk in order to successfully conduct business.

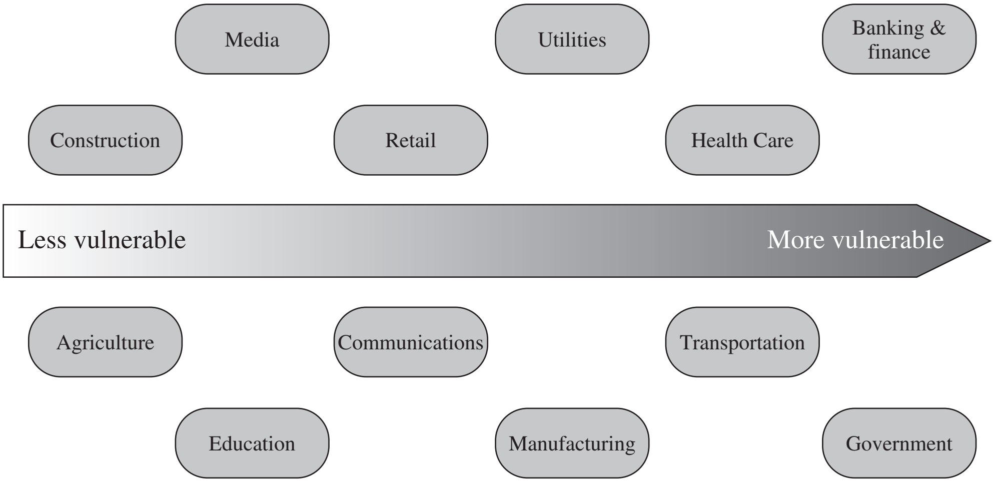

Figure 16.4 **Generic Organizational Risk Context**

[3] Reported in SANS NewsBites, 8(69), Sept. 1 2006.

Next, senior management must define the organization's **risk appetite**, the level of risk the organization views as acceptable. Again this will depend very much on the type of organization and its management's attitude to how it conducts business. For example, banking and finance organizations tend to be fairly conservative and risk averse. This means they want a low residual risk and are willing to spend the resources necessary to achieve this. In contrast, a leading edge manufacturer with a brand new product may have a much greater risk tolerance. The manufacturer is willing to take a chance to obtain a competitive advantage, and with limited resources wishes to expend less on risk controls. This decision is not just IT specific. Rather it reflects the organization's broader management approach to how it conducts business.

The boundaries of this risk assessment are then identified. This may range from just a single system or aspect of the organization to its entire IT infrastructure. This will depend in part on the risk assessment approach being used. A combined approach requires separate assessments of critical components over time as the security profile of the organization evolves. It also recognizes that not all systems may be under control of the organization. In particular, if services or systems are provided externally, they may need to be considered separately. The various stakeholders in the process also need to be identified, and a decision must be made as to who conducts and monitors the risk assessment process for the organization. Resources must be allocated for the process. This all requires support from senior management, whose commitment is critical for the successful completion of the process.

A decision also needs to be made as to precisely which risk assessment criteria will be used in this process. While there is broad general agreement on this process, the actual details and tables used vary considerably and are still evolving. This decision may be determined by what has been used previously in this, or related, organizations. For government organizations, this decision may be specified by law or regulation. Lastly, the knowledge and experience of those performing the analysis may determine the criteria used.

Asset Identification The last component of this first step in the risk assessment is to identify the assets to examine. This directly addresses the first of the three fundamental questions we opened this chapter with: "What assets do we need to protect?" An asset is "anything that needs to be protected" because it has value to the organization and contributes to the successful attainment of the organization's objectives. As we discuss in Chapter 1, an asset may be either tangible or intangible. It includes computer and communications hardware infrastructure, software (including applications and information/data held on these systems), the documentation on these systems, and the people who manage and maintain these systems. Within the boundaries identified for the risk assessment, these assets need to be identified and their value to the organization assessed. It is important to emphasize again that while the ideal is to consider every conceivable asset, in practice this is not possible. Rather the goal here is to identify all assets that contribute significantly to attaining the organization's objectives and whose compromise or loss would seriously impact on the organization's operation.

While the risk assessment process is most likely being managed by security experts, they will not necessarily have a high degree of familiarity with the organization's operation and structures. Thus they need to draw on the expertise of the people in the relevant areas of the organization to identify key assets and their value to the organization. A key element of this process step is identifying and interviewing such personnel. Many of the standards listed previously include checklists of types of assets and suggestions for mechanisms for gathering the necessary information. These should be consulted and used. The outcome of this step should be a list of assets, with brief descriptions of their use by, and value to, the organization.

Identification of Threats/Risks/Vulnerabilities

The next step in the process is to identify the threats or risks the assets are exposed to. This directly addresses the second of our three fundamental questions: "How are those assets threatened?" It is worth commenting on the terminology used here. The terms *threat* and *risk*, while having distinct meanings, are often used interchangeably in this context. There is considerable variation in the definitions of these terms, as seen in the range of definitions provided in the cited standards. [ISO13335] includes the following definitions:

Asset: anything that has value to the organization

Threat: a potential cause of an unwanted incident which may result in harm to a system or organization

Vulnerability: a weakness in an asset or group of assets which can be exploited by a threat

Risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

The relationship among these and other security concepts is illustrated in Figure 1.2, which shows that central term *risk* results from a threat exploiting vulnerabilities in assets that causes loss of value to the organization.

The goal of this stage is to identify potentially significant risks to the assets listed. This requires answering the following questions for each asset:

1. Who or what could cause it harm?
2. How could this occur?

Threat Identification Answering the first of these questions involves identifying potential threats to assets. In the broadest sense a threat is anything that might hinder or prevent an asset from providing appropriate levels of the key security services: confidentiality, integrity, availability, accountability, authenticity, and reliability. Note that one asset may have multiple threats, and a single threat may target multiple assets.

A threat may be either natural or human made and may be accidental or deliberate. This is known as the **threat source**. The classic natural threat sources are those often referred to as acts of God, and include damage caused by fire, flood, storm, earthquake, and other such natural events. It also includes environmental threats such as long-term loss of power or natural gas. Or it may be the result of chemical contamination or leakage. Alternatively, a threat source may be a human agent acting either directly or indirectly. Examples of the former include an insider retrieving and selling information for personal gain or a hacker targeting the organizations server over the Internet. An example of the latter includes someone writing and releasing a network worm that infects the organization's systems. These examples all involved a deliberate exploit of a threat. However, a threat may also be a result of an accident, such as an employee incorrectly entering information on a system, which results in the system malfunctioning.

Identifying possible threats and threat sources requires the use of a variety of sources, along with the experience of the risk assessor. The chance of natural threats occurring in any particular area is usually well known from insurance statistics. Lists of other potential threats may be found in the standards, in the results of IT security surveys, and in information from government security agencies. The annual computer crime surveys, such as those conducted by the CSI/FBI in the United States and AusCERT in Australia, provide useful general guidance on the broad IT threat environment and the most common problem areas.

However, this general guidance needs to be tailored to the organization and the risk environment it operates in. This involves consideration of vulnerabilities in the organization's IT systems, which may indicate that some risks are either more or less likely than the general case. The possible motivation of deliberate attackers in relation to the organization should be considered as potentially influencing this variation. In addition, any previous experience of attacks seen by the organization needs to be considered, as that is concrete evidence of risks that are known to occur. When evaluating possible human threat sources, it is worth considering their reason and capabilities for attacking this organization, including their

- **Motivation:** Why would they target this organization; how motivated are they?
- **Capability:** What is their level of skill in exploiting the threat?
- **Resources:** How much time, money, and other resources could they deploy?
- **Probability of attack:** How likely and how often would your assets be targeted?
- **Deterrence:** What are the consequences to the attacker of being identified?

Vulnerability Identification Answering the second of these questions, "How could this occur?", involves identifying flaws or weaknesses in the organization's IT systems or processes that could be exploited by a threat. This will help determine the applicability of the threat to the organization and its significance. Note that the mere existence of some vulnerability does not mean harm will be caused to an asset. There must also be a threat source for some threat that can exploit the vulnerability for harm. It is the combination of a threat and a vulnerability that creates a risk to an asset.

Again, many of the standards listed previously include checklists of threats and vulnerabilities and suggestions for tools and techniques to list them and to determine their relevance to the organization. The outcome of this step should be a list of threats and vulnerabilities, with brief descriptions of how and why they might occur.

Analyze Risks

Having identified key assets and the likely threats and vulnerabilities they are exposed to, the next step is to determine the level of risk each of these poses to the organization. The aim is to identify and categorize the risks to assets that threaten the regular operations of the organization. Risk analysis also provides information to management to help managers evaluate these risks and determine how best to treat them. Risk analysis involves first specifying the likelihood of occurrence of each identified threat to an asset, in the context of any existing controls. Next, the consequence to the organization is determined, should that threat eventuate. Lastly, this information is combined to derive an overall risk rating for each threat. The ideal would be to specify the likelihood as a probability value and the consequence as a monetary cost to the organization should it occur. The resulting risk is then simply given as

$$\text{Risk} = \text{Probability that threat occurs} \times \text{Cost to organization}$$

This can be directly equated to the value the threatened asset has for the organization, and hence specify what level of expenditure is reasonable to reduce the probability of its occurrence to an acceptable level. Unfortunately, it is often extremely hard to determine accurate probabilities, realistic cost consequences, or both. This is particularly true of intangible assets, such as the loss of confidentiality of a trade secret. Hence most risk analyses use qualitative, rather than quantitative, ratings for both these items. The goal is then to order the resulting risks to help determine which need to be most urgently treated, rather than give them an absolute value.

Analyze Existing Controls Before the likelihood of a threat can be specified, any existing controls used by the organization to attempt to minimize threats need to be identified. Security controls include management, operational, and technical processes and procedures that act to reduce the exposure of the organization to some risks, by reducing the ability of a threat source to exploit some vulnerabilities. These can be identified by using checklists of existing controls and by interviewing key organizational staff to solicit this information.

Determine Likelihood Having identified existing controls, the likelihood that each identified threat could occur and cause harm to some asset needs to be specified. The likelihood is typically described qualitatively, using values and descriptions such as those shown in Table 16.2.[4] While the various risk assessment standards all suggest tables similar to these, there is considerable variation in their detail.[5] The selection of the specific descriptions and tables used is determined at the beginning of the risk assessment process, when the context is established.

There will very likely be some uncertainty and debate over exactly which rating is most appropriate. This reflects the qualitative nature of the ratings, ambiguity in their precise meaning, and uncertainty over precisely how likely it is that some threat may eventuate. It is important to remember that the goal of this process is to provide guidance to management as to which risks exist and provide enough information to

[4] This table, along with Tables 16.3 and 16.4, is adapted from those given in [ADSD06], [SASN04], and [SA04], but with descriptions expanded and generalized to apply to a much wider range of organizations.

[5] The tables used in this chapter are chosen to illustrate a more detailed level of analysis than used in some other standards. For example, [NIST02] includes similar tables, though using a much smaller range of values.

Table 16.2 Risk Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may deemed as "unlucky" or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

help management decide how to most appropriately respond. Any uncertainty in the selection of ratings should be noted in the discussion on their selection, but ultimately management will make a business decision in response to this information.

The risk analyst takes the descriptive asset and threat/vulnerability details from the preceding steps in this process and, in light of the organization's overall risk environment and existing controls, decides the appropriate rating. This estimation relates to the likelihood of the specified threat exploiting one or more vulnerabilities to an asset or group of assets, which results in harm to the organization. The specified likelihood needs to be realistic. In particular, a rating of likely or higher suggests that this threat has occurred sometime previously. This means past history provides supporting evidence for its specification. If this is not the case, then specifying such a value would need to be justified on the basis of a significantly changed threat environment, a change in the IT system that has weakened its security, or some other rationale for the threat's anticipated likely occurrence. In contrast, the Unlikely and Rare ratings can be very hard to quantify. They are an indication that the threat is of concern, but whether it could occur is difficult to specify. Typically such threats would only be considered if the consequences to the organization of their occurrence are so severe that they must be considered, even if extremely improbable.

Determine Consequence/Impact on Organization The analyst must then specify the consequence of a specific threat eventuating. Note this is distinct from, and not related to, the likelihood of the threat occurring. Rather, consequence specification indicates the impact on the organization should the particular threat in question actually eventuate. Even if a threat is regarded as rare or unlikely, if the organization would suffer severe consequence should it occur, then it clearly poses a risk to the organization. Hence, appropriate responses must be considered. A qualitative descriptive value, such as those shown in Table 16.3, is typically used to describe the consequence. As with the likelihood ratings, there is likely to be some uncertainty as to the best rating to use.

This determination should be based upon the judgment of the asset's owners, and the organization's management, rather than the opinion of the risk analyst. This

Table 16.3 Risk Consequences

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4–8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

is in contrast with the likelihood determination. The specified consequence needs to be realistic. It must relate to the impact on the organization as a whole should this specific threat eventuate. It is not just the impact on the affected system. It is possible that a particular system (a server in one location, for example) might be completely destroyed in a fire. However, the impact on the organization could vary from it being a minor inconvenience (the server was in a branch office, and all data were replicated elsewhere), to a major disaster (the server had the sole copy of all customer and financial records for a small business). As with the likelihood ratings, the consequence ratings must be determined knowing the organization's current practices and arrangements. In particular, the organization's existing backup, disaster recovery, and contingency planning, or lack thereof, will influence the choice of rating.

Table 16.4 Risk Level Determination and Meaning

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Determine Resulting Level of Risk Once the likelihood and consequence of each specific threat have been identified, a final level of risk can be assigned. This is typically determined using a table that maps these values to a risk level, such as those shown in Table 16.4. This table details the risk level assigned to each combination. Such a table provides the qualitative equivalent of performing the ideal risk calculation using quantitative values. It also indicates the interpretation of these assigned levels.

Documenting the Results in a Risk Register The results of the risk analysis process should be documented in a **risk register**. This should include a summary table such that shown in Table 16.5. The risks are usually sorted in decreasing

Table 16.5 Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet router	Outside hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of data center	Accidental fire or flood	None (no disaster recovery plan)	Unlikely	Major	High	2

order of level. This would be supported by details of how the various items were determined, including the rationale, justification, and supporting evidence used. The aim of this documentation is to provide senior management with the information needed to make appropriate decisions as how to best manage the identified risks. It also provides evidence that a formal risk assessment process has been followed if needed, and a record of decisions made with reasons for those decisions.

Evaluate Risks

Once the details of potentially significant risks are determined, management needs to decide whether it needs to take action in response. This would take into account the risk profile of the organization and its willingness to accept a certain level of risk, as determined in the initial *Establishing the Context* phase of this process. Those items with risk levels below the acceptable level would usually be accepted with no further action required. Those items with risks above this will need to be considered for treatment.

Risk Treatment

Typically the risks with the higher ratings are those that need action most urgently. However, it is likely that some risks will be easier, faster, and cheaper to address than others. In the example risk register shown in Table 16.5, both risks were rated High. Further investigation reveals that a relatively simple and cheap treatment exists for the first risk, by tightening the router configuration to further restrict possible accesses. Treating the second risk requires developing a full disaster recovery plan, a much slower and more costly process. Hence management would take the simple action first, to improve the organization's overall risk profile as quickly as possible. Management may even decide that for business reasons, given an overall view of the organization, some risks with lower levels should be treated ahead of other risks. This is a reflection of both limitations in the risk analysis process in the range of ratings available and their interpretation and management's perspective of the organization as a whole.

Figure 16.5 indicates a range of possibilities for costs versus levels of risk. If the cost of treatment is high but the risk is low, then it is usually uneconomic to proceed with such treatment. Alternatively, where the risk is high and the cost comparatively low, then clearly treatment should occur. The most difficult area occurs between these extremes. This is where management must make a business decision about the most effective use of available resources. This decision usually requires a more detailed investigation of the treatment options. There are five broad alternatives available to management for treating identified risks:

- **Risk acceptance:** Choosing to accept a risk level greater than normal for business reasons. This is typically due to excessive cost or time needed to treat the risk. Management must then accept responsibility for the consequences to the organization should the risk eventuate.
- **Risk avoidance:** Not proceeding with the activity or system that creates this risk. This usually results in loss of convenience or ability to perform some function that is useful to the organization. The loss of this capability is traded off against the reduced risk profile.

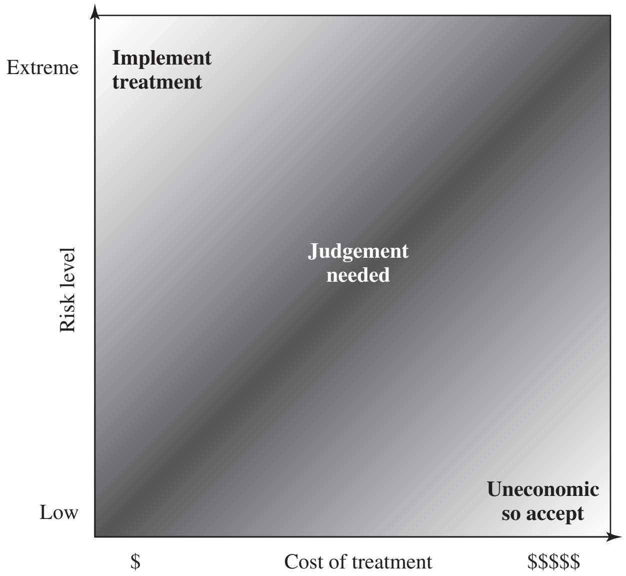

Figure 16.5 **Judgment about Risk Treatment**

- **Risk transferal:** Sharing responsibility for the risk with a third party. This is typically achieved by taking out insurance against the risk occurring, by entering into a contract with another organization, or by using partnership or joint venture structures to share the risks and costs should the threat eventuate.
- **Reduce the consequence:** By modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur. This could be achieved by implementing controls to enable the organization to quickly recover should the risk occur. Examples include implementing an off-site backup process, developing a disaster recovery plan, or arranging for data and processing to be replicated over multiple sites.
- **Reduce the likelihood:** By implementing suitable controls to lower the chance of the vulnerability being exploited. These could include technical or administrative controls such as deploying firewalls and access tokens, or procedures such as password complexity and change policies. Such controls aim to improve the security of the asset, making it harder for an attack to succeed by reducing the vulnerability of the asset.

If either of the last two options is chosen, then possible treatment controls need to be selected and their cost effectiveness evaluated. There is a wide range of available management, operational, and technical controls that may be used. These would be surveyed to select those that might address the identified threat most effectively and to evaluate the cost to implement against the benefit gained. Management would then choose among the options as to which should be adopted and plan for their implementation. We discuss the range of control often used and the use of security plans and policies in Chapter 17.

16.5 CASE STUDY: SILVER STAR MINES

A case study involving the operations of a fictional company Silver Star Mines illustrates this risk assessment process.[6] Silver Star Mines is the local operations of a large global mining company. It has a large IT infrastructure used by numerous business areas. Its network includes a variety of servers, executing a range of application software typical of organizations of its size. It also uses applications that are far less common, some of which directly relate to the health and safety of those working in the mine. Many of these systems used to be isolated, with no network connections among them. In recent years they have been connected together and connected to the company's intranet to provide better management capabilities. However, this means they are now potentially accessible from the Internet, which has greatly increased the risks to these systems.

A security analyst was contracted to provide an initial review of the company's risk profile and to recommend further action for improvement. Following initial discussion with company management, a decision was made to adopt a *combined approach* to security management. This requires the adoption of suitable baselines standards by the company's IT support group for their systems. Meanwhile, the analyst was asked to conduct a preliminary formal assessment of the key IT systems to identify those most at risk, which management could then consider for treatment.

The first step was to determine the context for the risk assessment. Being in the mining industry sector places the company at the less risky end of the spectrum, and consequently less likely to be specifically targeted. Silver Star Mines is part of a large organization and hence is subject to legal requirements for occupational health and safety and is answerable to its shareholders. Thus management decided that it wished to accept only moderate or lower risks in general. The boundaries for this risk assessment were specified to include only the systems under the direct control of the Silver Star Mine operations. This excluded the wider company intranet, its central servers, and its Internet gateway. This assessment is sponsored by Silver Star's IT and engineering managers, with results to be reported to the company board. The assessment would use the process and ratings described in this chapter.

Next, the key assets had to be identified. The analyst conducted interviews with key IT and engineering managers in the company. A number of the engineering managers emphasized how important the reliability of the SCADA network and nodes were to the company. They control and monitor the core mining operations of the company and enable it to operate safely and efficiently and, most crucially, to generate revenue. Some of these systems also maintain the records required by law, which are regularly inspected by the government agencies responsible for the mining industry. Any failure to create, preserve, and produce on demand these records would expose the company to fines and other legal sanctions. Hence, these systems were listed as the first key asset.

[6] This example has been adapted and expanded from a 2003 study by Peter Hoek. The name of the original company and any identifying details have been changed by request.

A number of the IT managers indicated that a large amount of critical data was stored on various file servers either in individual files or in databases. They identified the importance of the integrity of these data to the company. Some of these data were generated automatically by applications. Other data were created by employees using common office applications. Some of this needed be available for audits by government agencies. There were also data on production and operational results, contracts and tendering, personnel, application backups, operational and capital expenditure, mine survey and planning, and exploratory drilling. Collectively, the integrity of stored data was identified as the second key asset.

These managers also indicated that three key systems—the Financial, Procurement, and Maintenance/Production servers—were critical to the effective operation of core business areas. Any compromise in the availability or integrity of these systems would impact the company's ability to operate effectively. Hence each of these were identified as a key asset.

Lastly, the analyst identified e-mail as a key asset, as a result of interviews with all business areas of the company. The use of e-mail as a business tool cuts across all business areas. Around 60% of all correspondence is in the form of e-mail, which is used to communicate daily with head office, other business units, suppliers, and contractors as well as to conduct a large amount of internal correspondence. E-mail is given greater importance than usual due to the remote location of the company. Hence the collective availability, integrity, and confidentiality of mail services was listed as a key asset.

This list of key assets is seen in the first column of Table 16.6, which is the risk register created at the conclusion of this risk assessment process.

Table 16.6 Silver Star Mines—Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	Layered firewalls & servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	Firewall, policies	Possible	Major	Extreme	2
Availability and integrity of financial system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	3
Availability and integrity of procurement system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	4
Availability and integrity of maintenance/ production system	Attacks/errors affecting system	Firewall, policies	Possible	Minor	Medium	5
Availability, integrity, and confidentiality of mail services	Attacks/errors affecting system	Firewall, ext. mail gateway	Almost Certain	Minor	High	6

Having determined the list of key assets, the analyst needed to identify significant threats to these assets and to specify the likelihood and consequence values. The major concern with the SCADA asset is unauthorized compromise of nodes by an external source. These systems were originally designed for use on physically isolated and trusted networks and hence were not hardened against external attack to the degree that modern systems can be. Often these systems are running older releases of operating systems with known insecurities. Many of these systems have not been patched or upgraded because the key applications they run have not been updated or validated to run on newer O/S versions. More recently, the SCADA networks have been connected to the company's intranet to provide improved management and monitoring capabilities. Recognizing that the SCADA nodes are very likely insecure, these connections are isolated from the company intranet by additional firewall and proxy server systems. Any external attack would have to break through the outer company firewall, the SCADA network firewall, and these proxy servers in order to attack the SCADA nodes. This would require a series of security breaches. Nonetheless, given that the various computer crime surveys suggest that externally sourced attacks are increasing and known cases of attacks on SCADA networks exist, the analyst concluded that while an attack was very unlikely, it could still occur. Thus a likelihood rating of Rare was chosen. The consequence of the SCADA network suffering a successful attack was discussed with the mining engineers. They indicated that interference with the control system could have serious consequences as it could affect the safety of personnel in the mine. Ventilation, bulk cooling, fire protection, hoisting of personnel and materials, and underground fill systems are possible areas whose compromise could lead to a fatality. Environmental damage could result from the spillage of highly toxic materials into nearby waterways. Additionally, the financial impact could be significant, as down time is measured in tens of millions of dollars per hour. There is even a possibility that Silver Star's mining license might be suspended if the company was found to have breached its legal requirements. A consequence rating of Major was selected. This results in a risk level of High.

The second asset concerned the integrity of stored information. The analyst noted numerous reports of unauthorized use of file systems and databases in recent computer crime surveys. These assets could be compromised by both internal and external sources. These can be either the result of intentional malicious or fraudulent acts, or the unintentional deletion, modification, or disclosure of information. All indications are that such database security breaches are increasing and that access to such data is a primary goal of intruders. These systems are located on the company intranet and hence are shielded by the company's outer firewall from much external access. However, should that firewall be compromised or an attacker gain indirect access using infected internal systems, compromise of the data was possible. With respect to internal use, the company had policies on the input and handling of a range of data, especially that required for audit purposes. The company also had policies on the backup of data from servers. However, the large number of systems used to create and store this data, both desktop and server, meant that overall compliance with these policies was unknown. Hence a likelihood rating of Possible was chosen. Discussions with some of the company's IT managers revealed that some of this information is confidential and may cause financial harm if disclosed to others. There also may be substantial financial costs involved with recovering data and other activities subsequent to a breach. There is also the possibility of serious legal consequences if personal information was disclosed or if the results of statutory tests and process information were lost. Hence a consequence rating of Major was selected. This results in a risk level of Extreme.

The availability or integrity of the key Financial, Procurement, and Maintenance/Production systems could be compromised by any form of attack on the operating system or applications they use. Although their location on the company intranet does provide some protection, due to the nature of the company structure a number of these systems have not been patched or maintained for some time. This means at least some of the systems would be vulnerable to a range of network attacks if accessible. Any failure of the company's outer firewall to block any such attack could very likely result in compromise of some systems by automated attack scans. These are known to occur very quickly, with a number of reports indicating that unpatched systems were compromised in less than 15 minutes after network connection. Hence a likelihood of Possible was specified. Discussions with management indicated that the degree of harm would be proportional to extent and duration of the attack. In most cases a rebuild of at least a portion of the system would be required, at considerable expense. False orders being issued to suppliers or the inability to issue orders would have a negative impact on the company's reputation and could cause confusion and possible plant shutdowns. Not being able to process personnel time sheets and utilize electronic funds transfer, as well as unauthorized transfer of money would also affect the company's reputation and possibly result in a financial loss. The company indicated that the Maintenance/Production system's harm rating should be a little lower due the ability of the plant to continue to operate despite some compromise of the system. It would, however, have a detrimental impact on the efficiency of operations. Consequence ratings of Moderate and Minor, respectively, were selected, resulting in risk levels of High or Medium.

The last asset is the availability, integrity, and confidentiality of mail services. Without an effective e-mail system, the company will operate with less efficiency. A number of organizations have suffered failure of their e-mail systems as a result of mass e-mailed worms in recent years. New exploits transferred using e-mail are reported. Those exploiting vulnerabilities in common applications are of major concern. The heavy use of e-mail by the company, including the constant exchange and opening of e-mail attachments by employees, means the chance of compromise, especially by a zero-day exploit to a common document type, is very high. While the company does filter mail in its Internet gateway, there is a high probability that a zero-day exploit would not be caught. A denial-of-service attack against the mail gateway is very hard to defend against. Hence a likelihood rating of Almost Certain was selected in recognition of the wide range of possible attacks and the high chance that one will occur sooner rather than later. Discussions with management indicated that while other possible modes of communication exist, they do not allow for transmission of electronic documents. The ability to obtain electronic quotes is a requirement that must be met to place an order in the purchasing system. Reports and other communications are regularly sent via this e-mail, and any inability to send or receive such reports might affect the company's reputation. There would also be financial costs and time needed to rebuild the e-mail system following a serious compromise. Because compromise would not have a large impact, a consequence rating of Minor was selected. This results in a risk level of High.

The information was summarized and presented to management. All of the resulting risk levels are above the acceptable minimum management specified as tolerable. Hence treatment is required. Even though the second asset listed had the highest level of risk, management decided that the risk to the SCADA network was unacceptable if there was any possibility of death, however remote. Additionally, management decided that the government regulator would not look favorably upon a company that failed to rate highly the importance of a potential fatality. Consequently, management decided to specify the risk to the SCADA as the highest priority for treatment. The risk to the integrity of stored information was next. Management also decided to place the risk to the e-mail systems last, behind the lower risk to the maintenance/production system, in part because its compromise would not affect the output of the mining and processing units and also because treatment would involve the company's mail gateway, which was outside management's control.

The final result of this risk assessment process is shown in Table 16.6, the resulting overall risk register table. It shows the identified assets with the threats to them and the assigned ratings and priority. This information would then influence the selection of suitable treatments. Management decided the first five risks should be treated by implementing suitable controls, which would reduce either the likelihood or the consequence should these risks occur. This process is discussed in the next chapter. None of these risks could be accepted or avoided. Responsibility for the final risk to the e-mail system was found to be primarily with the parent company's IT group, which manages the external mail gateway. Hence the risk is shared with that group.

16.6 RECOMMENDED READING AND WEB SITES

[SLAY06] provides a discussion issues involved with IT security management. [SCHN00] provides a very readable, general discussion of IT security issues and myths in the modern world. Current best practice in the field of IT Security Management is codified in a range of international and national standards, whose use is encouraged. These standards include [ISO17799], [ISO27001], [ISO13335], [ADSD06], [SASN04], [SA04], [NIST95], and [NIST02].

ADSD06 Australian Defence Signals Directorate, "ACSI33—Australian Communications—Electronic Security Instruction 33," ISB DSD, 2006.

ISO13335 ISO/IEC, "ISO/IEC 13335–1:2004—Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management." Part 2 on operational guidance for ICT security management will be released soon.

ISO17799 ISO/IEC, "ISO/IEC 17799:2005—Information technology—Security techniques—Code of practice for information security management." Will be replaced by ISO27002.

ISO27001 ISO/IEC, "ISO/IEC 27001:2005—Information technology—Security Techniques—Information security management systems—Requirements." This replaces the older Australian and British national standards AS7799.2 and BS7799.2.

NIST95 National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800–12. October 1995.

NIST02 National Institute of Standards and Technology. *Risk Management Guide for Information Technology Systems*. Special Publication 800–30. July 2002.

SA04 Standards Australia, "HB 231:2004—Information Security Risk Management Guidelines." 2004.

SASN04 Standards Australia and Standards New Zealand, "AS/NZS 4360:2004: Risk Management." 2004.

SCHN00 Schneier, B. *Secrets & Lies—Digital Security in a Networked World*, New York: John Wiley & Sons, 2000.

SLAY06 Slay, J., and Koronios, A. *Information Technology Security & Risk Management*. Milton, Qld: John Wiley & Sons Australia, 2006.

Recommended Web sites:

- **AusCERT—Australian Computer Crime and Security Surveys**: Details of the annual surveys of computer network attacks and computer misuse trends in Australia each year
- **ISO 27000 Directory**: An overview of the ISO 27000 series of standards reserved by ISO for information security matters
- **ISO 27001 Security**: Dedicated to providing information on the latest international standards for information security

16.7 KEY TERMS, REVIEW QUESTIONS, AND PROBLEMS

Key Terms

asset
consequence
control
countermeasure
IT security management
level of risk
likelihood
organizational security policy
risk
risk appetite
risk assessment
risk register
security attack
security mechanism
security objectives
threat
threat source
vulnerability

Review Questions

16.1 Define *IT security management*.

16.2 List the three fundamental questions IT security management tries to address.

16.3 List the steps in the process used to address the three fundamental questions.

16.4 List some of the key national and international standards that provide guidance on IT security management and risk assessment.

16.5 List and briefly define the four steps in the iterative security management process.

16.6 Organizational security objectives identify what IT security outcomes are desired, based in part on the role and importance of the IT systems in the organization. List some questions that help clarify these issues.

16.7 List and briefly define the four approaches to identifying and mitigating IT risks.

16.8 Which of the four approaches for identifying and mitigating IT risks does [ISO13335] suggest is the most cost effective for most organizations?

16.9 List the steps in the detailed security risk analysis process.

16.10 Define *asset*, *control*, *threat*, *risk*, and *vulnerability*.

16.11 Indicate who provides the key information when determining each of the key assets, their likelihood of compromise, and the consequence should any be compromised.

16.12 State the two key questions answered to help identify threats and risks for an asset. Briefly indicate how these questions are answered.

16.13 Define *consequence* and *likelihood*.

16.14 What is the simple equation for determining risk? Why is this equation not commonly used in practice?

16.15 What are the items specified in the risk register for each asset/threat identified?

16.16 List and briefly define the five alternatives for treating identified risks.

Problems

16.1 Research the IT security policy used by your university or by some other organization you are associated with. Identify which of the topics listed in Section 16.2 this policy addresses. If possible, identify any legal or regulatory requirements that apply to the organization. Do you believe the policy appropriately addresses all relevant issues? Are there any topics that the policy should address but does not?

16.2 As part of a formal risk assessment of desktop systems in a small accounting firm with limited IT support, you have identified the asset “integrity of customer and financial data files on desktop systems” and the threat “corruption of these files due to import of a worm/virus onto system.” Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

16.3 As part of a formal risk assessment of the main file server for a small legal firm, you have identified the asset “integrity of the accounting records on the server” and the threat “financial fraud by an employee, disguised by altering the accounting records”. Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

16.4 As part of a formal risk assessment of the external server in a small web design company, you have identified the asset “integrity of the organization’s web server” and the threat “hacking and defacement of the web server”. Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

16.5 As part of a formal risk assessment of the main file server in an IT security consultancy firm, you have identified the asset “confidentiality of techniques used to conduct penetration tests on customers, and the results of conducting such tests for clients, which are stored on the server” and the threat “theft/breach of this confidential and sensitive information by either an external or internal source.” Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

16.6 As part of a formal risk assessment on the use of laptops by employees of a large government department, you have identified the asset "confidentiality of personnel information in a copy of a database stored unencrypted on the laptop" and the threat "theft of personal information, and its subsequent use in identity theft caused by the theft of the laptop." Suggest reasonable values for the items in the risk register for this asset and threat, and provide justifications for your choices.

16.7 As part of a formal risk assessment process for a small public service agency, suggest some threats that such an agency is exposed to. Use the checklists provided in the various risk assessment standards cited in this chapter to assist you.

16.8 Compare [NIST02] Tables 3.4 to 3.7, which specify levels of likelihood, consequence, and risk, with Tables 16.2 to 16.4 in this chapter. What are the key differences? What is the effect on the level of detail in risk assessments using these alternate tables?