Box 1.2 *Continued...*

reported as one of the most effective solutions. However, a limitation of the TP monitor technology is that the implementation code is usually written in a lower level language (such as COBOL), and is not yet widely available in the popular visual toolsets.

1.5 Globalization of Businesses and the Need for Distributed Information Systems

Liberalization, privatization and globalization have become the three 'mantras' of success in the digital economy led by the rise of e-business. Business competition and pressures are on the rise like never before. Businesses now have no geographical boundaries. With the rise of mobile commerce (m-commerce) fuelled by mobile technologies, we are now witnessing the era of *anywhere anytime computing*! Naturally, 'information' that has been one of the vital corporate resources (in addition to the traditional '3Ms', i.e., man, materials and money) assumes a higher dimension when it comes to data and information security (InfoSec). In the paradigm of mobile computing, information as a vital corporate resource has the threat of falling in the hands of those for whom it is not intended. Protecting the data and information is crucial as businesses make knowledge-based decisions. We certainly do not want the confidential data and information to be leaked outside the required boundaries.

We talked about the 'waves' in the previous section. There is an important point to be noted – while the industrial age witnessed great developments in terms of engineering, a significant dimension, connectivity, was missing. Producers and consumers of goods all remained disparate and unconnected. They operated in islands of geographical pockets without knowing how the others were transacting their businesses. This isolation is not true anymore in today's paradigm of 'extended enterprise' resulting from the new way of doing the business, namely the electronic business or, popularly known as, 'e-business'. So, prior to e-business days, not only did the suppliers and consumers remain separated, but the knowledge producers/knowledge workers and business personnel also remained relatively unconnected.

The 'third wave' has what the 'second wave' did not have: connectivity. Connectivity is a great boon from the 'Internet' – one of the most exciting revolutions of this century and truly a paradigm changing force. Connectivity in the Information Age not only brought the consumers and producers together, but also built the bridge between the 'thinkers', business people, the governments, the common people, the academicians and so on. We need to consider at the scope of modern-day IS in this global context.

In the new paradigm, IS are handling information in all forms, not just the text-based data of the 1970s that came typically in flat files but also the rich text, images/graphics and voice. So, we are in the realm of not only terabytes of data but also multimedia, multi-geo order of IS. The widening scope of IS can be summarized as follows:

1. **1950s:** technical changes;
2. **1960s–1970s:** managerial controls;
3. **1980s–1990s:** institutional core activities;
4. **Today:** digital information webs extending beyond the enterprise.

Today's firms are 'digital' in terms of their rapid operations mode. They are characterized by electronic commerce (e-commerce) and e-business to operate in the 'digital market' where IS link the buyers and sellers to exchange information, products, services and payments. Thus, today, the era is of the 'extended enterprise' and to serve the needs of such networked enterprises; the IS, too, are no more confined to a single location, single computer. Figure 1.7 shows the wider boundaries of the modern information system vis-à-vis the past.

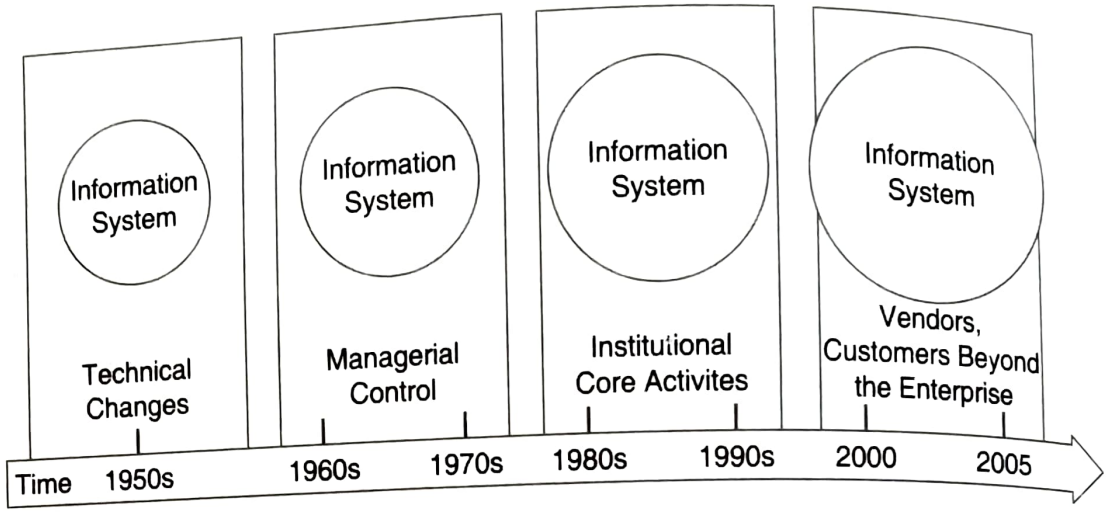


Figure 1.7 | The wider scope of information systems.

1.6 Global Information Systems: Role of Internet and Web Services

The Internet, one of the most marvelous inventions of this century, in fact, a 'killer application', is the international network of networks. The Internet is a universal technology platform that allows any computer to communicate with any other computer in the world. Furthermore, one of the advantages of the Internet is that nobody really 'owns' it. It is a global collection of networks, both big and small. These networks connect together in many different ways to form the single entity that we know as the Internet. In fact, the very name comes from this idea of interconnected networks as shown in Figure 1.8.

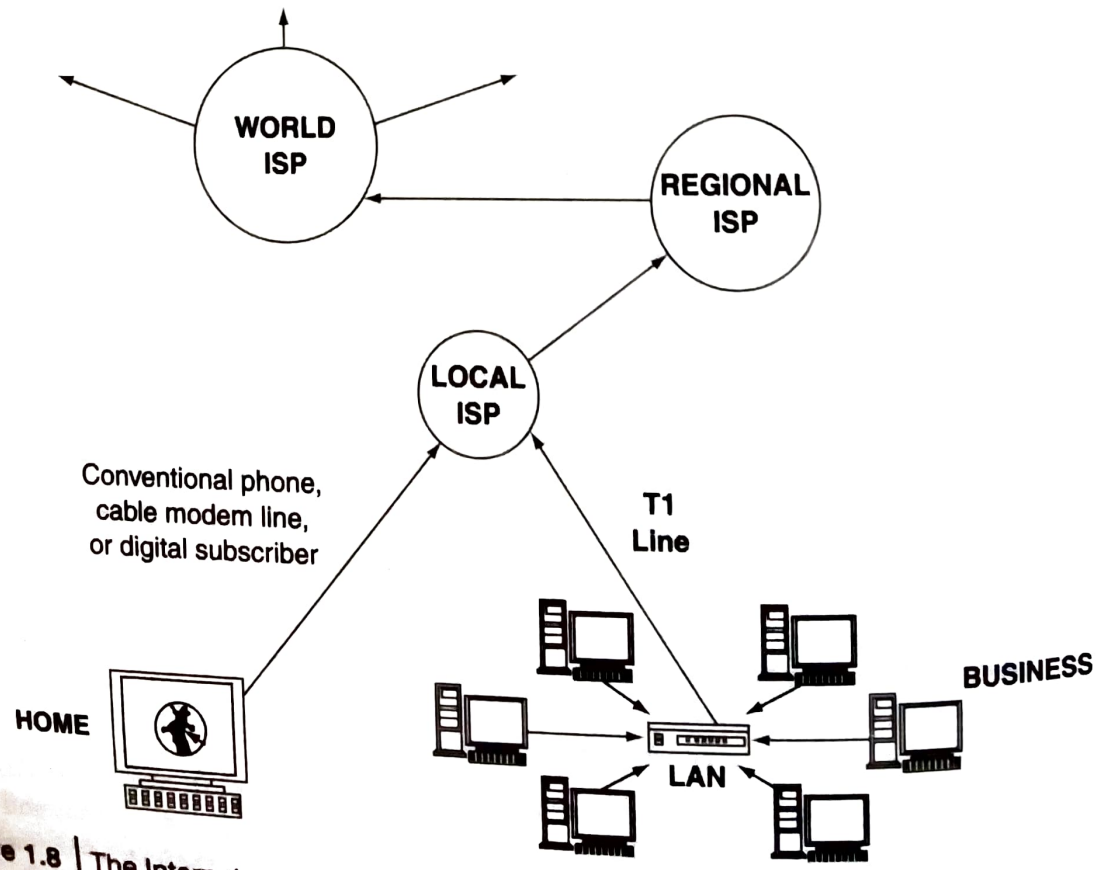


Figure 1.8 | The Internet.

The Internet has become so well-meshed in the day-to-day working of the knowledge workers that its contribution is acknowledged by everybody. Although the Internet, indeed, has brought the world closer in a way, this very 'free' and 'autonomous' nature of the Internet does have some implications for the security of IS as we will see later. In this section, we focus on the contribution of web services to modern IS in the global .

The Internet has revolutionized communication and thereby its contribution to information sharing. With access to a computer and an appropriate connection, anyone can interact with others worldwide. However, the web is designed to exchange unstructured information: while people can read web pages and understand their meaning, computers cannot. If corporations want to conduct business over the web, humans have to be involved unless there is a way for computers to communicate on their own. This is where *web services* come in. They make it possible for companies to do business through their computer systems exploiting the Internet infrastructure.

Web services play a complementary and dominant role in building global IS for today's dynamic business world. IBM's definition of web services states that 'Web Services are self-contained, modular applications that can be described, published, located and invoked over a network, generally, the World Wide Web (WWW).' Companies send and receive a great deal of information, by automating even a small part. However, one of the greatest benefits from web services comes from links between companies, where extended processes between companies can be automated. This is very much essential in the paradigm of today's 'extended enterprise concept' (Figure 1.2).

Web services perform functions ranging from simple requests to complicated business processes. Once a web service is developed, other applications and other web services can discover and invoke the deployed service through universal description, discovery and integration (UDDI). The idea of web services is to leverage the advantages of the web as a platform to apply it to the services themselves, not just to the static information. 'Services' refer to components and the services offered that can be used to build larger application services. Web services make it easier to build service-based architectures without the applications being locked-in to a particular software vendor's products.

Web services have been proven to give a strong return on investment (ROI) and make computer-based IS more adaptable. They also help bring productivity, flexibility and low maintenance cost in the development of IS by integrating components from various third-party vendors (another avenue for implementing appropriate security measures in the IS). Web services make information available from computer systems to other applications using well-defined standards (see Box 1.3). Discussion on the details of standards adopted in web services is beyond the scope of this book. Interested readers can refer to web services-related topics provided in *Further Reading* section.

Box 1.3 Web Services Standards

Common object request broker architecture (CORBA®) and electronic data interchange (EDI) were created as single specifications, but web service vendors are adopting a series of standards that work together. In general, these standards can handle specific tasks. The advantage of this approach is that web service standards can evolve more easily as new requirements are identified.

The first standards to be agreed upon concern basic interoperation among applications, and since then, a series of standards have covered web services discovery, security, transactions and coordination. There is also a body, the Web Services Interoperability Organization (WS-I), charged with overseeing the establishment and promulgation of standards. The standards include:

1. *simple object access protocol* (SOAP), used to format messages between web services;
2. *web services definition language* (WSDL), used to define how a web service can be used;

Box 1.3 *Continued...*

3. *universal description, discovery and integration* (UDDI) and *the web services inspection language* (WSIL), used to find web services;
4. *WS-security*, used to manage *security across web services*;
5. *WS-coordination*, used to *coordinate multiple web services* into a larger composite system.

Many other web service standards remain under development. Organizations that publish these standards include the *World Wide Web Consortium* (W3C) and the *Organization for the Advancement of Structured Information Standards* (OASIS).

Benefits of web services for developing IS of global nature are as follows:

1. Web services tools are available for most computer systems, including mainframes and packaged applications. This means that not only the existing applications can be retained, but also the existing knowledge of staff can be applied and extended using web services for business integration.
2. Web services are adaptable and can handle changes more readily than other integration solutions because they use structured text as their message format. Therefore, because the cost of maintenance is reduced, the overall cost of a web services system also reduces.
3. IT managers now have the ability to exchange data between most applications, on most computers, in a consistent and standard way. Tools and further standards are therefore emerging to build composite applications that can model and manage business processes around these business-level components.
4. If necessary, an alternative application can be used to provide web services without changing the overall effect of the system. This gives significant flexibility in the choice of a supplier. This aspect is particularly important in the consideration of outsourcing security services.

1.7 Information Systems Security and Threats: A Glimpse

So far, we have seen that the use of IS has become mandatory for businesses to perform their day-to-day functions efficiently. In this section, we set the context for understanding the issues related to IS misuse, resulting threats and countermeasures. This section is only an overview about threats to IS. It sets the stage for the detailed discussion taken up in the next chapter on the role of organization in security management.

Given the crucial role played by information systems, it is important that they remain secured and that the data contained in them do not fall into the hands of those who are not intended to have access to it. Security of IS becomes particularly important with the advent of the Internet. The access by Internet in particular allows a mass of information to remain up-to-date in real time, but it also opens the door for external encroachment. Thus, it is essential to ensure the physical protection of the information that, when stored without precautions on the hard disk of a computer connected to the Internet, can be read, copied, modified or destroyed from a working station located somewhere on the planet without the owner realizing the tampering.

In the modern business era, the use of desktop PCs, laptops, and network connectivity including the Internet and electronic mail (e-mail) is as essential as the telephone at workplace. The employees and networked IS are the most valuable assets for any organization. The misuse of information systems by employees, however, poses serious challenges to organizations including loss of productivity, loss of revenue, legal liabilities and other workplace issues. Organizations need effective countermeasures to enforce their appropriate usage policies and minimize their losses as well as increase the productivity of knowledge workers. The basics of *information systems security* are related to:

1. Trademark, copyright, patent and trade secrets and protection strategies for each of them (discussion on this is available in Chapter 38);
2. Software licensing issues (Chapter 37 has discussion on software license management);
3. Data privacy under legal framework (Laws and Legal Frameworks are addressed in Chapter 27. Data Privacy fundamentals are addressed in Chapter 29);
4. InfoSec and control frameworks such as Control Objective for Information and related Technology (COBIT) and International Organization for Standardization (ISO) 17799 (COBIT is addressed in Chapter 25 and the ISO 17799 framework is addressed in Chapter 23);
5. Evidence of digital forensic practices and ethics;
6. Computer Frauds and Abuse Acts boundaries for illegal access to computers/computer-based IS;
7. Electronic surveillance and cyber crimes.

InfoSec measures are mandated by statutes such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, Gramm–Leach–Bliley Act (GLBA) and Sarbanes–Oxley Act (SOX) (because most Indian IT/software firms have majority of their business with the United States, it is important to include this). HIPAA, GLBA and SOX are addressed in Chapter 27.

Summary

Information systems play a crucial role in today's complex business world. They have come a long way progressing from the precivilization era, through the agricultural era, to the present networked enterprise era in our digital economy. To fulfill the demands placed on them, today's IS are global in nature and complex in their structure. Information is an important asset and needs to be protected all the time. Threats to IS come from many avenues and these threats will continue, given our dependence on information system. In the next chapter, an organizational context is set for managing information systems security.

Review Questions

1.1 Explain the historical role of information systems. In what way do you think, the industrial revolution impacted information systems?

1.2 Explain the importance of information systems in the global context. Do you think that only computer-based information systems will be successful today? Give reasons for your argument.

1.3 Do you feel geographical limits play a role in the effective working of information systems? Give reasons.

1.4 Explain the 'extended enterprise concept'. In what way information systems play the cementing role among the various components of the extended enterprise? Elaborate your answer with suitable examples.

1.5 What are the factors that alter today's enterprises? Have information systems changed over the years? In what way have they changed and what challenges does this present to the designers of information system? Explain with illustrations.

1.6 Explain the various architectures for information systems as described in this chapter.

1.7 How do distributed information systems help the global enterprises?

1.8 Explain the crucial role of the Internet and Web Services.

1.9 What elements, as described in this chapter, form the basics of information systems security?

2 Threats to Information Systems

Learning Objectives

After completing this chapter you will be able to:

- understand how new technologies can pose threats to information systems.
- distinguish information-level threats from network-level threats
- understand information systems security in terms of threats and attacks.
- know about nuisance value of computer viruses.
- classify threats to assess damages to information systems.
- understand logical and physical types of assets; this will be useful later for understanding the concepts in Chapter 37 about asset management.
- re-assimilate the need for safeguarding information systems security.
- learn about information systems controls.

2.1 Introduction

Information systems security is the integrity and safety of its resources and activities. In the cyber world, it can be almost impossible to trace sophisticated attacks to their true source. The anonymity enjoyed by today's cyber attackers poses a grave threat to the global information society, the progress of an information-based international economy and the advancement of global collaboration and cooperation in all areas of human endeavor.

In Chapter 1, we discussed about the strategic importance of information systems (IS) and their role in the global context. In this chapter, our objective is to provide a context for management role and responsibility for ensuring the security of IS in the organization. To achieve this, our focus in this chapter is to provide an overview of 'threats to IS'. In Chapter 4, we take up a discussion on security management in organizations and the role of security policies and procedures in this, to counter the threats to IS.

2.2 New Technologies Open Door to the Threats

For companies in the modern era, in particular those engaged in electronic business (e-business), it is increasingly important to be aware of the online threats because more and more people are using the Internet to access information about their (prospective) business partners, customers and other business-related links. In today's world, almost all business organizations have IS that use integrated technologies such as the networks of computers, company intranets or Internet access to communicate and transmit information for rapid business decisions, thereby opening the organization to the external world like never before. Under these circumstances, threats from outside the organization must be addressed, because the damages from non-secured information system can result in catastropic consequences for the organization.

Given this, organizations must investigate and evaluate the factors that could be a threat to the integrity of the information system. Box 2.1 provides some snippets on what can happen while using electronic emails (e-mails) and the Internet.

Box 2.1 Threatening Online Activities

Hacking of computer systems and launching of denial of service (DoS) attacks as well as spreading of malicious code, such as viruses, are well-known online threats that deserve attention in the computer security and security management domain. Far less attention is provided to the fact that the Internet has enabled a range of potentially threatening activities that are based on the active or passive dissemination of certain information. Examples of such information-based threatening activities are:

1. **Myths, rumors and hoaxes:** Hoaxes are false e-mail messages with the only purpose to spread to as many people as possible. Along with myths and urban legends, they live on the Internet. Such messages may have significant impact on companies, their reputations and thus on their businesses.
   More recently, the globally operating mobile phone company Ericsson was the victim of a hoax promising recipients free mobiles if they forward the letter to at least 20 people. Ericsson received thousands of e-mail from people asking for their free phones. The article (Park, 2000) quotes an Ericsson Australia spokesman claiming that the company was aware of the e-mail circulating for at least a couple of days and that the way it was sent makes it impossible for them to see where the e-mail originated from.
   Another report (Fumento, 1999) has the story about a Canadian manufacturer who used his/her website to spread information that products of competitors may be dangerous. Moreover, the company's marketing head has been observed to actively support feminists preparing a petition to start a boycott of the company's competitors. According to Fumento (1999), however, scientific investigations suggest that the information is nothing but a myth.
2. **Threats to websites:** There are reports that the US-based car manufacturer Ford decided not to go online to combat a certain revenge website as the company was afraid that anything they would do on their own website would validate what is described on the revenge website!
3. **Limited attention to cyber crimes:** So far, threats on the information level, referred by lawyers as 'commercial terrorism through the Internet', have not received much attention in the computer security and security management literature. A look at the relevant literature suggests that these fields tend to focus on making corporate computer systems and networks secure in order to protect systems. Interested readers may like to refer to the paper by Lueg (2001).

2.3 Information-Level Threats versus Network-Level Threats

As a reference to the discussion in the rest of this chapter, we describe three basic terms: *threat*, *vulnerability* and *countermeasures*. A threat is a possible event that can harm an information system, whereas vulnerability is the degree of exposure in view of a threat. Finally, a countermeasure is a set of actions implemented to prevent threats. Next, let us consider a working definition of information-level threats. Information-level threats (or information-based threats) are threats that involve the (purposeful) dissemination of information in such a way that organizations, their operations and their reputations may be affected. Dissemination may be active as in the case of sending an e-mail or it may be passive as in the case of setting up websites (see Box 2.1).

It is important to distinguish 'information-level threats' from 'network-level threats'. By network-based threats we mean that in order to become effective, potential attackers require network access to corporate

computer systems or to networks used by corporate computer systems. Examples for network-based threats (or threats on the network layer) are hacking of computer systems and launching of DoS attacks as well as spreading malicious code, such as viruses (more on this topic in Section 2.5). Other security issues involved when data are transmitted over networks are *confidentiality, authentication, integrity* and *non-repudiation* (these terms are discussed in detail in Chapter 5).

Information-level threats also make heavy use of network but at the primary level is the content of a message and not its form. Sending fake inquiries to service accounts to eat up resources (e.g., flooding the mail server with many messages so that it gets choked) would qualify as an information-based attack – as it is the content of the messages that would provide a basis for the attack. Other examples of information-based threats are setting up revenge websites and disseminating false or biased information as in the case of the false accusation (see Box 2.1). Such attacks can cause considerable damage to the goodwill of the organization against which they may be launched, and customer loyalty is too good to lose.

Dissemination of information that is likely to trigger specific counter-reactions as in the case of say some falsified job advertisement also qualifies as information-based threat. Essentially, a DoS attack that is based on flooding accounts with large quantities of e-mail is a network-based attack as it is the size and the quantity of the e-mail that matters and not the content of the e-mail.

2.4 Information Systems Security: Threats and Attacks

Attacks can be represented by the relation among threat, vulnerability and damage. Threat and vulnerability have already been defined. Before the rise of Internet and the increase in the number of connections from and to the outside, threats were mainly physical ones (intrusion into the company premises without authorization, robberies, vandalism, etc.). Protection could be summed up in a very few access control rules using, for example, multi-locks and security guards. Nowadays the situation is quite different. Admittedly, there are still thefts of equipment or intrusion through the main console. Attacks via the network have reached a critical point and companies still do not know what the best measures to be taken are.

The above discussion brings us to classifying information systems security threats. Security threats have four principal sources that include:

1. **Human error:** for example, inadvertent disclosure of confidential information.
2. **Computer abuse or crime:** these days crime is rampant. A generic example is when a person intends to be malicious and starts to steal information from sites, or cause damage to, a computer or computer network. In particular, consider these examples; An Internet-based computer fraud can happen when a victim is expecting a large payoff for helping to move millions of dollars out of a foreign country. The victim may also believe s/he has won a large award in a non-existent foreign lottery. In the US, for example, 'wire-fraud' is a specific form of computer-related crime where the means of communications is a central feature of the offence, credit card data from hacked websites, password-sniffing programs used to obtain information required to gain access to the password owner's system.
3. **Natural and political disasters:** this can happen in the form of natural calamities and wars, riots, etc.
4. **Failure of hardware or software:** for example, server malfunctioning, software errors, etc.

Computer crime is defined as any illegal act in which a computer is used as the primary tool. Computer abuse is unethical use of a computer. Security threats related to computer crime or abuse include:

1. **Impersonation:** The impersonator enjoys the privileges of a legitimate user by gaining access to a system by identifying oneself as another person after having defeated the identification and authentication controls employed by the system.

2. **Trojan horse method:** Concealing within an authorized program a set of instructions that will cause unauthorized actions.
3. **Logic bomb:** Unauthorized instructions, often introduced with the Trojan horse technique, which stay dormant until a specific event occurs (or until a specific time comes, as the instructions may keep checking the computer's internal clock), at which time they bring into effect an unauthorized act.
4. **Computer viruses:** Segments of code that are able to perform malicious acts and insert copies of themselves into other programs in the system and onto the diskettes placed in the computer. Because of this replication, a virus will progressively infect healthy programs and systems. Close relatives of viruses are *worms* – independent programs that make and transmit copies of themselves through telecommunications (TC) networks. Computer viruses have become a pervasive threat in personal computing.
5. **DoS:** Rendering the system unusable by legitimate users.
6. **Dial diddling:** Changing data before or during input, often to change the contents of a database.
7. **Salami technique:** Diverting small amounts of money from a large number of accounts maintained by the system. These small amounts will not be noticed.
8. **Spoofing:** Configuring a computer system to masquerade as another system over the network in order to gain unauthorized access to the resources the system being mimicked is entitled to.
9. **Super-zapping:** Using a system's program that can bypass regular system controls to perform unauthorized acts.
10. **Scavenging:** Unauthorized access to information by searching through the residue after a job has been run on a computer. Techniques range from searching wastebaskets or dumpsters for printouts to scanning the contents of a computer's memory.
11. **Data leakage:** There are a variety of methods for obtaining the data stored in a system. The data may be encoded into an innocuous report in sophisticated ways, for example, as the number of characters per line.
12. **Wiretapping:** Tapping computer TC lines to obtain information.
13. **Theft of mobile devices:** This is a new dimension that is coming up given the increase in mobile workforce.

Some of the above-mentioned crime techniques may be used for a direct gain of financial resources, others for industrial espionage, while yet others simply for destructive purposes. Probably the most important unrecognized threat today is the theft of portable computers, with access codes and information in their memories. Also to be considered are the losses owing to the theft of intellectual property, such as software, product development information, customer information or internal corporate documents. Chapter 3 is devoted to discuss security issues in the mobile computing arena.

Box 2.2 Signaling Under Attack: History

The world of security threats has given rise to some interesting terms. For example, take the term 'phone-phreakers'. The term phone-phreaking refers to attack on signaling. Until the 1980s, phone companies used signaling systems that worked in-band by sending tone pulses in the same circuit that carried the speech. The first signaling attack dates back to 1952. By the mid-to-late 1960s, many phone-phreakers in both United States and Britain had worked out ways of routing calls. They typically used homemade tone generators, called the 'blue boxes'. The trick they used was the following: call an 800 (toll free) number, and then send a tone that would clear down the line at the far end, that is, disconnect the called party while leaving the caller with a trunk line connected to the exchange. The caller could now enter the number s/he really wanted and be connected without paying.

Box 2.2 *Continued...*

According to some analysts (Diffe and Landau, 1998), there are at least as many unauthorized wiretaps as authorized ones. The figures can be distorted from country to country, depending on the level of controls to prevent illegal practices in wiretapping. Even if the official figures have to be doubled or tripled, it is still clear that democratic regimes make very less use of wiretapping compared to the authoritarian ones. For example, lawful wiretapping amounted to 63,243 line-days in the United States in 1999, or an average of just over 173 taps in place.

Another point worth noting is that the incidence of wiretapping is highly variable in the developed democracies. In the United States, for example, it is found that only about half the states use wiretapping. In Britain, wiretaps need a ministered warrant, and so are rarer. The cost of wiretapping is a serious issue. This raises some obvious policy questions: Should agencies cut back on wiretapping, and spend more money on deployment of civil crime investigation squads?

2.5 Computer Viruses: The *bête noire* of Computing Era

Computer viruses deserve a special attention in the sense that they are really the 'black beasts' of modern computing era! They are the most frequently encountered threats to end-user computing and are the best-known form of computer threat. A computer virus is a piece of program code that attaches copies of itself to other programs and thus replicates itself. Computer viruses possess certain characteristics:

1. The attacked program may work properly, but, at some point, will perform a malicious or destructive act intended by the attacker who has written the virus.
2. Although a computer virus may attack a multi-user system with shared disk facilities, viruses are best known for their rapid spread in a personal computer (PC) environment. In this environment, they proliferate through infected diskettes or programs downloaded from the Internet or other networks.
3. Most viruses are insidious and their presence is not obvious after the infection. In the meantime, they infect other programs.
4. Two principal types of viruses are boot infectors and program infectors. Boot infectors replace the contents of the first sector of the diskette or hard disk. These are the viruses that most commonly occur in personal computing. Program infectors copy themselves into the executable files stored on the hard disk.

2.6 Classifications of Threats and Assessing Damages

So far we have discussed the threats to IS. Discussion in this section forms the basis for understanding security management in an organization in terms of security policies, security architectures and security procedures/processes. This will also serve as a foundation for a discussion on disaster recovery planning (DRP) and business continuity planning (BCP) in Chapter 34. Also, we will see later, preventive measures are the best to avoid threats. However, even after all this, since we do not operate in a foolproof and ideal world, things may still go wrong and then the next action is to get into a recovery mode. Organizations expect that their security managers are in a position to evaluate the damage caused when a security incident or an actual attack takes place so that the management can draw the budget for security-related spending. For this, it is important that the threat and resulting damages are categorized. Security managers need to know explicitly about the assets of their organizations, the vulnerability of their IS to different threats and their potential damages.

A threat is an indication of a potential undesirable event. It refers to a situation in which a person could do something undesirable (e.g., an attacker initiating a DoS attack against an organization's e-mail server) or in which a natural occurrence could cause an undesirable outcome (e.g., a fire damaging an organization's information technology (IT) hardware). Threats consist of the following properties (note that this maps to the fourth source of security threats mentioned in Section 2.4):

1. **Asset:** something of value to the organization (information in electronic or physical form, IS, a group of people with unique expertise, etc.).
2. **Actor:** who or what may violate the security requirements – confidentiality, integrity, and availability (CIA) – of an asset. Actors can be from inside or outside the organization.
3. **Motive (optional):** indication of whether the actor's intentions are deliberate or accidental.
4. **Access (optional):** how the asset will be accessed by the actor (network access or physical access).
   - **Outcome:** the immediate result of violating the security requirements of an asset (disclosure, modification, destruction, loss, interruption, etc.).

   The major categories of damages resulting from threats to the IS are:
   - destruction of information and/or other resources;
   - corruption or modification of information;
   - theft, removal or loss of information and/or other resources;
   - disclosure of information (confidential data);
   - modification of important or sensitive information;
   - interruption of access to important information, software, applications or services.

Each threat and vulnerability must be related to one or more of the organizational assets requiring protection. Thus, prior to assessing damages (caused by security incidents), we need to identify assets. Typically, there are five categories of logical and physical assets:

1. **Information:** documented (paper or electronic) data or intellectual property used to meet the mission of an organization.
2. **Software:** software applications and services that process, store or transmit information.
3. **Hardware:** IT physical devices considering their replacement costs.
4. **People:** the people in an organization who possess skills, competencies, knowledge and experience that are difficult to replace.
5. **Systems:** IS that process and store information (conceptually, a system is a combination of information, software and hardware assets. In computer networking terms, any host, client or server also can be considered a system).

Another way of grouping the threats is to put them together in groups based on some common themes suggested as follows:

1. **Human actors using network access:** The threats in this category are network-based threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
2. **Human actors using physical access:** The threats in this category are physical threats to an organization's critical assets. They require direct action by a person and can be deliberate or accidental in nature.
3. **System problems:** The threats in this category are problems with an organization's IT systems. Examples include hardware defects, software defects, unavailability of related enterprise systems, viruses, malicious code and other system-related problems.

4. **Other problems:** The threats in this category are problems or situations that are outside the control of an organization. This category of threats includes natural disasters (such as floods, earthquakes and storms) that can affect an organization's IT systems as well as interdependency risks. Interdependency risks include the unavailability of critical infrastructures (TC, electricity, etc.). Other types of threats outside the control of an organization can also be included here. Examples of these threats are power outages, broken water pipes, etc.

Thus, we can see that threat profiles can be represented as a tree structure. This structure depicted in Figure 2.1 that shows the assets, access, actors, motives and the possible outcomes. An important point to notice is that organizations should have a suitable method for 'asset classification' to know which of their assets are critical.

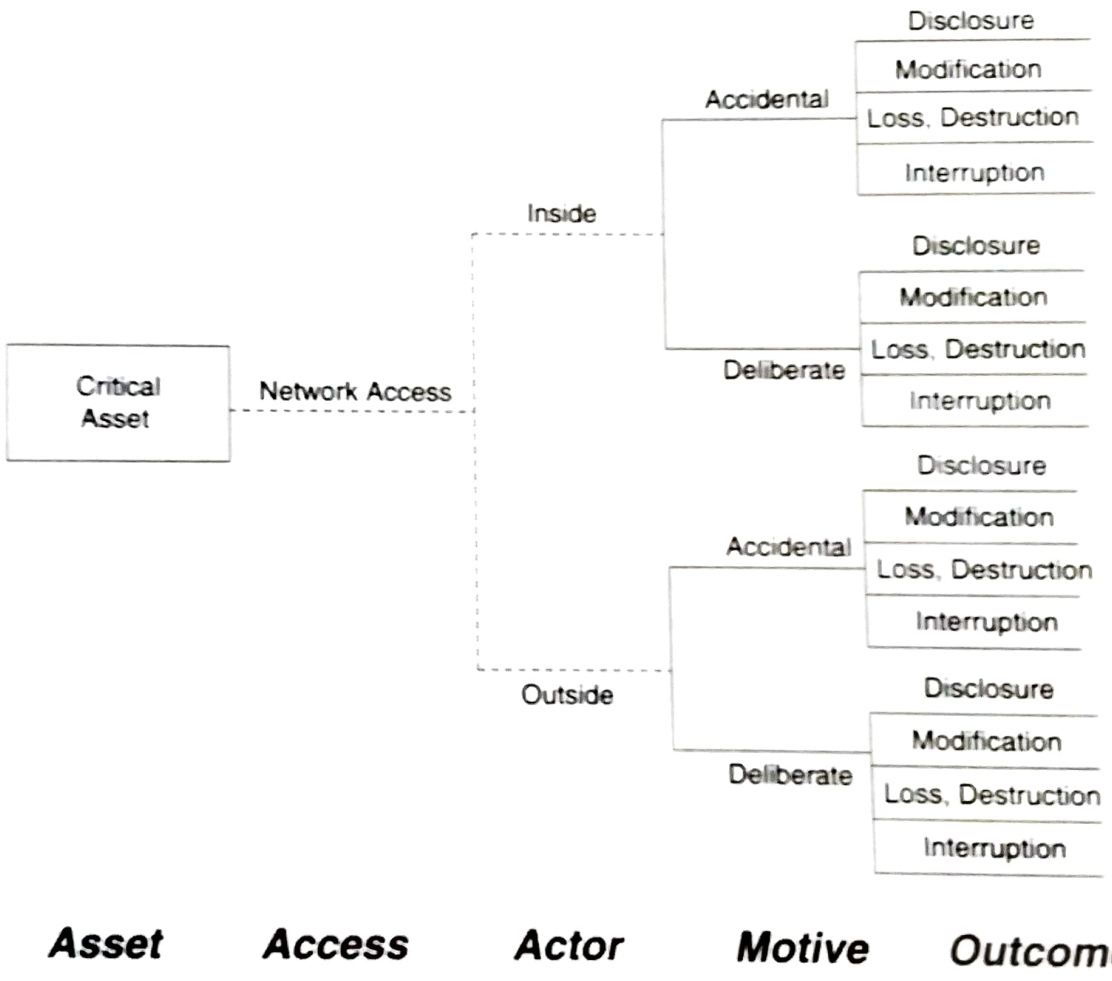


Figure 2.1 | Generic threat profile.

Organizational assets are evaluated using various suitable units of measurements. Monetary value of assets is the most commonly used unit. It is not always easy to measure assets in absolute terms. In such cases, measurement for assessment of damages can be done in relative ways, for example, information. The value of information can be measured as a fraction or percentage of total budget, assets or worth of a business in relative fashion. Assets may also be ranked by sensitivity or importance to an organization in relative ways.

The impact of information security (InfoSec) incidents may well be financial, in form of immediate costs and losses of assets. For example, the cost of downtime per hour caused by a DoS attack can be computed by measuring the loss of:

1. **Productivity:** (number of employees impacted) × (hours wasted) × (burdened hourly rate). Note that burdened hourly rate could be the notional cost of the employees – for example, billing rate of the employees to the customer or in terms of their outgoing cost to the employing organization (salary of the employees).
2. **Revenue:** direct loss and lost future revenues.
3. **Financial performance:** credit rating and stock price.
4. **Other expenses:** equipment rental, overtime costs, extra shipping costs, travel expenses, etc.

Hidden costs are difficult to handle. Consider the example of a DoS attack (this situation was illustrated in Box 2.1) where the damaged reputation of the company can have a negative impact on the relationship of the company with its customers, suppliers, financial markets, banks and business partners. These hidden costs are extremely difficult to quantify and measure. The bottom line is that the cost of an information systems security incident in a company has to be measured in terms of the impact on its business; hence, identical incidents in two different companies can have different costs. To evaluate these costs and measure the impact of a security incident on a company, organizations need a systematic approach and a comprehensive risk management system. A discussion on this is taken up in Chapter 6.

Box 2.3 Reason for Security Breaches

IS and networks are often inherently insecure because they are designed with functionality, not security, as their primary goal. Most organizations view security threats as inbound, that is from outside to inside. However, there are major threats to security that are introduced not by external sources but by employees themselves (see Figure 2.1). It is important that organizations understand the inside threats and extend perimeter security controls to local desktops with security measures such as host-based intrusion detection system (IDS), personal firewall and anti-virus software.

1. **Employee issues and social engineering:** With easy availability of hacking tools, disgruntled employees can find ingenious ways of unauthorized access to corporate confidential data. Security breaches can even happen owing to accidental risk of attaching wrong files in e-mail attachment or sending e-mail to wrong recipient. This shows why policies about e-mail usage are so important.
   Social engineering attacks can trick legitimate, though naive, users into providing them with access to corporate systems. Sharing folders on a PC, choosing weak passwords, sharing passwords, leaving important printouts on desk and not locking the screens are some of the examples of lack of sense of security, due care and diligence. Whether the origin of such incidents is malicious intent or inadvertent employee error, the result is the same: loss of revenue, productivity and potential liability.
2. **Rise in mobile workers:** Prevalence of laptops and wireless connectivity to the Internet has only compounded the security control problems for organizations. The mobile workers using laptops at homes without appropriate controls (as per organizational guidelines) may introduce viruses, worms or offensive content into the corporate network when they connect their laptops at workplace. The use of laptops also poses significant exposure of an organization's confidential information when it gets out of the organization network. Therefore, organizations must have appropriate mobile computing policies in place to protect their information assets.

2.7 Protecting Information Systems Security

The discussion in the previous section shows that the security of IS needs to be maintained by measures taken to prevent threats to these systems or to detect and correct the effects of any damage. The aim of

information systems security is to protect corporate assets or, at least, to limit their loss. Security measures limit the access to information to authorized individuals; there can be no privacy or confidentiality of data records without adequate security.

In view of the discussion so far in this chapter and Chapter 1, we need to understand that good InfoSec design starts with a threat model – what the system is designed to protect, from whom, and for how long. Threat modeling involves thinking about the system as a whole and imagining the vulnerability landscape. It must take into account the information to be protected, the people who will use the system as well as how they will use it. Whether external or internal, threats are opportunities that have the potential to cause harm or loss to organizations. As such, organizations need to adopt adequate measures to combat such threats to mitigate the resulting risks.

Information systems controls play a crucial role to ensure secure operations of IS and thus to safeguard assets and the data stored in these systems. Information systems controls need to be established to ensure that the business applications achieve their objectives in an efficient manner, and that organizations need to institute a set of policies, procedures and technological measures. Information systems controls are classified as follows:

1. **Preventive controls:** prevent an error or an attack from taking effect. These are designed to prevent or restrict an error, omission or unauthorized intrusion.
2. **Detective controls:** detect a violation. These controls exist to detect and report when errors, omissions and unauthorized use or entry occur.
3. **Corrective controls:** detect and correct an exceptional situation. These controls are designed to correct errors, omissions and unauthorized users and intrusions once they are detected.

Box 2.4 InfoSec Assurance Capability Maturity Model (IA-CMM)

Version 3.0, October 2003

The Systems Engineering Capability Maturity Model (SE-CMM) is Copyright © 1995 by Carnegie Mellon University and the Systems Security Engineering Capability Maturity Model (SSE-CMM) is held and maintained by the International System Security Engineering Association (ISSEA).

The IA-CMM contains 37 InfoSec assurance BASE Practices, organized into nine process areas (PAs) that address the specific performance of an InfoSec assurance activity. Each PA has a set of goals that represent the expected state of an organization that is successfully performing the PA. An organization that performs the base practices of the PA has to also achieve its goals.

PAs of the IA-CMM

The nine process areas of the IA-CMM are listed as follows:

1. **PA01:** provide training;
2. **PA02:** coordinate with customer organization;
3. **PA03:** specify initial InfoSec needs;
4. **PA04:** assess threat;
5. **PA05:** assess vulnerability;
6. **PA06:** assess impact;
7. **PA07:** assess InfoSec risk;
8. **PA08:** provide analysis and results;
9. **PA09:** manage InfoSec assurance processes.

For IA PA04: assess threat, the best practices are:

1. **IA-BP04.01:** identify applicable threats;
2. **IA-BP04.02:** identify threat impact potential;
3. **IA-BP04.03:** assess threat agent capability;
4. **IA-BP04.05:** monitor threats.

Box 2.4 *Continued...*

Information systems controls are classified as:

1. **General controls:** controls applying to the entire IS activity in the organization.
2. **Application controls:** controls that are specific to a given application (payroll). Application controls are employed at application security layer. This topic will be discussed in detail in reference to the security audit best practices.

From the preceding discussions we learn that, for protecting the IS, threats must be stood before effective InfoSec measures are devised. This is typically done through risk assessment for safeguarding IS. During risk assessment, vulnerabilities and threats are analyzed (this is discussed in detail in Chapter 6). We had mentioned four sources of security threats in Section 2.4; threats can be classified according to the way they can occur – non-fraudulent, that is accidental, and fraudulent, that is intentional. A more elaborate way to classify threats is to say that they can be fundamental, which represents what an attacker really wants to do: information disclosure, information tampering, DoS, repudiation and illegitimate use – for example, masquerade or authorization violation and underlying threats, for example, eavesdropping or administrative error.

Given the role of IS and threats to them, the matter of their security warrants senior management attention in an organization. This is so because, in addition to assuring protection against threats and compliance with certain legal requirements, InfoSec has evolved into a powerful tool for developing business solutions. Effective InfoSec promotes business objectives and expands business opportunities; therefore, InfoSec can be viewed as a business enabler. When managed effectively, InfoSec can deliver a competitive edge by generating new markets and revenue streams and leveraging new distribution channels. The nature and degree of threats faced by organizations vary; therefore, a risk assessment of the likelihood that security will be compromised is needed. An acceptable level of InfoSec can be introduced and maintained only if the set of security controls, procedural and technical, is correctly identified, implemented and maintained. These activities must be seen as a never-ending process. Furthermore, organizations should aim to gain an understanding of the specific characteristics of the emerging environment that may generate new threats. The consequences of failure to do so may severely impair their ability to carry out their business and may even lead to legal exposures and liabilities. This is where security policy plays a crucial role.

Summary

Information system is a unit that includes technologies, people and processes. Threats that organizations have to cope with are numerous and can have catastrophic consequences on the future of the organizations. The last few years have seen a proliferation of automated IS, reliance on the Internet to enable most of the essential services and infrastructures, and the growing threat of organized cyber attacks capable of causing debilitating disruption to our critical infrastructures. Proliferation of computers and networks in the age of the Internet has enabled not only novel services, such as e-mail, the web and electronic commerce (e-commerce), but also new ways to affect companies, their businesses and their reputations. The Internet has the potential to become an even greater threat to computer security than dial-up telephone modems. However, a look at the relevant literature suggests that information-level threats are not yet sufficiently addressed.

It is now widely acknowledged that security of computer-based IS is an important topic and the

state-of-the-art security tools can provide some protection against threats ranging from hackers trying to break into corporate computer systems to DoS attacks. Companies should be able to reduce vulnerabilities as well as the potential impact of still successful attacks. However, it is unlikely that there will ever be a 'security end state'. The situation is like accepting that software will be buggy; similarly, when it comes to IS, some levels of threats are always residual. There is a need for an equally important step toward a realistic assessment of computer security and toward a lasting change of attitudes and expectations. One of the most overlooked threats in a corporate security program is the threat posed by employee behavior. Prevention of the misuse of IS by employees has a direct business value. User awareness and training also play a role here. Controls and policies play a crucial role in mitigating threats to information systems security; although not fool-proof in themselves, they occupy a central role in information systems security management. This is a subject area that will be explored in the next chapter.

Review Questions

2.1 Explain how new technologies open doors to potential attackers on corporate information systems.

2.2 Distinguish between information-level threats and network-level threats.

2.3 Provide a scheme for classifying threats to information systems and the resulting damages.

2.4 Why are computer viruses considered as one of the major threats to computer systems?

2.5 What kind of thinking and approach should be applied by organizations for protecting their information system assets?

Further Reading

Bisson, J. and Saint-Germain, R. (2003) *The BS 7799 ISO 17799 Standard for a Better Approach to Information Security*, Callio Technologies White Paper.

Diffe, W. and Landau, S. (1998) *Privacy on the Line – The Politics of Wiretapping and Encryption*, MIT Press, Cambridge, MA, USA.

Farahmand, F., Navathe, S., Sharp, G.P. and Enslow, P.H. (2001–2002) *Evaluating Damages caused by Information Systems Security Incidents,* Georgia Institute of Technology, Atlanta, GA, USA.

Fumento, M. (1999) *Tampon terrorism in Forbes Global,* available at http://www.forbes.com/global/1999/0517/0210033a.html (accessed 1 January 2006).

Godbole, N. (2003) *Mobile Computing: Security Issues in Hand-Held Devices,* Paper presented at NASONES 2003 National Seminar on Networking and E-Security by Computer Society of India.

Godbole, N. and Unhelkar, B. (February 2006) *Security Issues in Mobile Computing*, Paper presented at the 2nd International Conference on Information Management and Business, Sydney, Australia.

Lueg, C. (2001) *The Role of Information Systems in Information Level Security Management,* Department of Information Systems, University of Technology Sydney, Sydney, Australia.

Park, B. (2000) *Free mobile phones offer a hoax, says Ericsson. IT News from The Age and the Sydney Morning Herald*, available at http://it.mycareer.com.au/breaking/20000407/A54797-2000Apr7.html (accessed 15 October 2001).

Vasiu, L., Mackay, D. and Warren, M. (2003) *The Tri-Dimensional Role of Information Security in e-Business: A Managerial Perspective, School of Information Technology*, Deakin University, Australia.

* **Refer case illustration 'Super Tech – IT Risk Assessment in an ERP Setup' on the CD companion of the book for a scenario based on the concept(s) discussed in this chapter.**

4 Information Security Management in Organizations

Learning Objectives

After completing this chapter you will be able to:

- understand the context for information security management.
- appreciate the role of security policies, standards, guidelines and procedures.
- learn about various types of security policies.
- know about InfoSec scenario in the financial sector.
- learn about information security management system (ISMS) as the foundation for InfoSec management.
- understand organization's responsibility towards information security management.
- get an overview of information security awareness in the industry.

4.1 The Context for Information Security Management (ISM)

In Chapter 2, we provided an overview of information systems security threats. In Chapter 3, the focus was on information security (InfoSec) risks brought in by mobile and wireless computing. In this chapter, the main focus is to understand who is responsible to provide information systems security in an organization, that is the role of management in information systems security.

The prime driver for enterprise security is Internet connectivity. According to International Data Corporation (IDC), the worldwide information security market was worth USD 6.7 billion in 2000. With a compounded annual growth rate (CAGR) of 25.5%, this market was projected to more than triple to USD 21 billion by the end of 2005. According to an IDC analyst, remote local area network (LAN), Internet, extranet/intranet and wireless access services will drive the need for advanced InfoSec services, as technologies for circumventing network security systems continue to keep pace with the technologies designed to defend against them. This provides us the context for the chapter. We use the context to learn about organization's responsibilities for managing InfoSec.

4.2 Security Policy, Standards, Guidelines and Procedures

Security Policy and Policy Types

We aim to discuss two important terms in this section: 'policy' as a general term along with various types of policies and the meaning of 'security policy'; as a specific term. A policy is one of those terms that can mean several things in the information security domain. For example, consider a firewall (Chapter 15 is dedicated to the discussion of firewalls). There are security policies on firewalls which refer

to the access control and routing list information. Note that even standards, procedures and guidelines are referred to as 'policies' in the larger sense of a global InfoSec policy. A well-written policy is more than an exercise created on paper – it is an essential and fundamental element of sound security practice. A policy, for example, can literally be a lifesaver during a disaster, or it might be a requirement of a governmental or regulatory function. A policy can also provide protection from liability owing to an employee's actions or can form a basis for the control of trade secrets.

Types of Policies

When the term 'policies' is used rather than 'policy', the intent is to refer to those policies that are distinct from the *standards*, *procedures* and *guidelines*; these terms are discussed in the next section with respect to the terms in Figure 4.4.

Figure 4.1 relates well to Figure 4.3. It shows that 'policies' are considered as the first and the highest level of documentation. Lower level elements of standards, procedures and guidelines flow from policies. However, this does not imply that the lower level elements are not important. It is just that the higher level policies, being general in nature, should be created first for strategic reasons and then the tactical elements should follow. With this brief introduction, we now list the policy types and then describe each briefly. Essentially, there are the following types of policies:

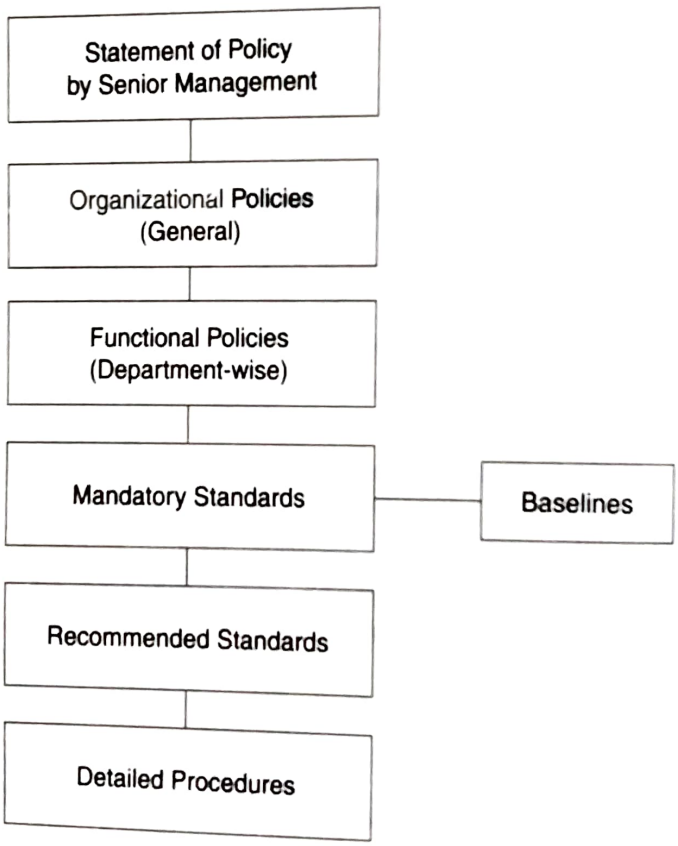


Figure 4.1 | Policy hierarchy chart.

1. **Senior management statement of policy:** This is the first step in the policy creation process. This is a general, high-level statement of policy that contains the following elements:
   - an acknowledgement of the importance of computing and networking resources, that are part of the information system, to the organization's business model;

- a statement of support for InfoSec throughout the business enterprise;
- a commitment to authorize and manage the definition of the lower level standards, procedures and guidelines.

2. **Regulatory policy:** These are security policies that an organization must implement owing to compliance, regulation or other legal requirements as prevalent in the organization's operating environment, both internal and external (e.g. as shown in Table 1.1 of Chapter1). The various entities with which the business organization interacts can be financial institutions (such as those in the banking sector), public utilities or some other types of organizations that operate in the public interest. Regulatory policies are usually very detailed and specific to the industry in which the business organization operates. The two main purposes of the regulatory policies are:
   - ensuring that an organization follows the standard procedures or base practices of an operation in its specific industry;
   - giving an organization the confidence that it is following the standard and accepted industry policy.
3. **Advisory policy:** These are security policies that may not be mandated but are strongly recommended. Normally, the consequences of not following them are defined (e.g., Business Conduct Guidelines in an organization – not following these could result in job termination). An organization with such policies wants its employees to consider these policies mandatory. Most policies fall under this broad category.
4. **Informative policy:** These are policies that exist simply to inform the reader. There are no implied or specified requirements, and the audience for this information could be certain internal entities (within the organization) or external parties.

Having discussed the term 'policy' in general, let us now turn to 'security policy'. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role security plays within the organization. A security policy, we will see in this chapter, can be an organizational policy, an issue-specific policy or a system-specific policy.

Security policy can be defined as a codified set of processes and procedures applied to secure the fulfillment of its obligations and the continuation of its activities even in the presence of possible interferences. This definition may appear to be vague as compared to the others that may be found in technical computer-related publications – it is actually crafted by choosing each word precisely. Security policies are most often referred to in the context of information technology (IT), telecommunications (TC) or information and communications technologies (ICTs). Moreover they are often, erroneously though, associated exclusively with the deployment of computer hardware or software and the configuration of the hardware or software, to the point of the 'configuration' being called security policy.

The definition given in the International Organization for Standardization (ISO) standard 17799 is a slightly different one: 'Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organisation'. *It should be remembered that ISO standard 17799 assumes an implicit definition of what is a policy, and a separate indication is provided about the necessity of a policy document including an indication of possible contents (not reproduced here)*: 'A policy document should be approved by management, published and communicated, as appropriate, to all employees'.

It must be pointed out that any other standard on security should not be applied or used in a mechanical way like a fixed formula, but rather it should be interpreted keeping in perspective the needs and working model of the 'entity' (e.g., business, non-profit organization, university, etc.) in which its application is planned, as well as the needs of the organization that created it. This is because in an organizational security policy, the management establishes how a security program will be set up, establishes the program's goals,

assigns responsibilities, shows the strategic and tactical value of security and outlines how enforcement should be carried out. Thus, the security policy must address prevalent laws and regulations as applicable as well as the liability issues that may arise and how they must be addressed to satisfy the statutory requirements. Box 4.1 shows the goals of security engineering as a discipline and Box 4.2 has the SSE-CMM PAs.

Box 4.1 Security Engineering Principles

Goals of Security Engineering

1. Understand security risks;
2. establish security needs;
3. develop security guidance (policies, standards, and procedures);
4. determine acceptable risks;
5. establish security assurance.

Who Practices Security Engineering?

1. Product developers;
2. product vendors;
3. product integrators;
4. product buyers;
5. security evaluation organizations;
6. system administrators;
7. consulting/IT service organizations;
8. program/project management teams.

Box 4.2 Security-Related Process Areas in Systems Security Engineering Capability Maturity Model (SSE–CMM) (Version 3.0)

The SSE-CMM provides a community-wide standard metric to establish and advance security engineering as a mature measurable discipline. It contains five levels of maturity (further depicted in Figure 4.2):

1. **level 1**: performed informally;
2. **level 2**: planned and tracked;
3. **level 3**: well defined;
4. **level 4**: quantitatively controlled;
5. **level 5**: continuously improving.

The Security Best Practices in the SSE–CMM are given in the following list of process areas (PAs):

1. **PA01:** administer security controls;
2. **PA02:** assess impact;
3. **PA03:** assess security risk;
4. **PA04**: assess threat;
5. **PA05:** assess vulnerability;
6. **PA06:** build assurance argument;
7. **PA07**: coordinate security;
8. **PA08**: monitor security posture;

Box 4.2 *Continued...*

9. **PA09**: provide security input;
10. **PA10**: specify security needs;
11. **PA11**: verify and validate security.

Figure 4.2 SSE-CMM document includes excerpts from 'A Systems Engineering Capability Maturity Model, Version 1.1', CMU/SEI-95-MM-003, published in November 1995. The SE-CMM, that is, Systems Engineering CMM is Copyright © 1995 by Carnegie Mellon University. This work is a collaborative effort of Hughes Space and Communications, Hughes Telecommunications and Space, Lockheed Martin, Software Engineering Institute (SEI), Software Productivity Consortium and Texas Instruments Incorporated. Permission to reproduce this product and to prepare derivative works from this product is granted royalty-free, provided the copyright is included with all reproductions and derivative works.
Courtesy: //www.sse.cmm.org, http://www.sse-cmm.org/model/model.asp.

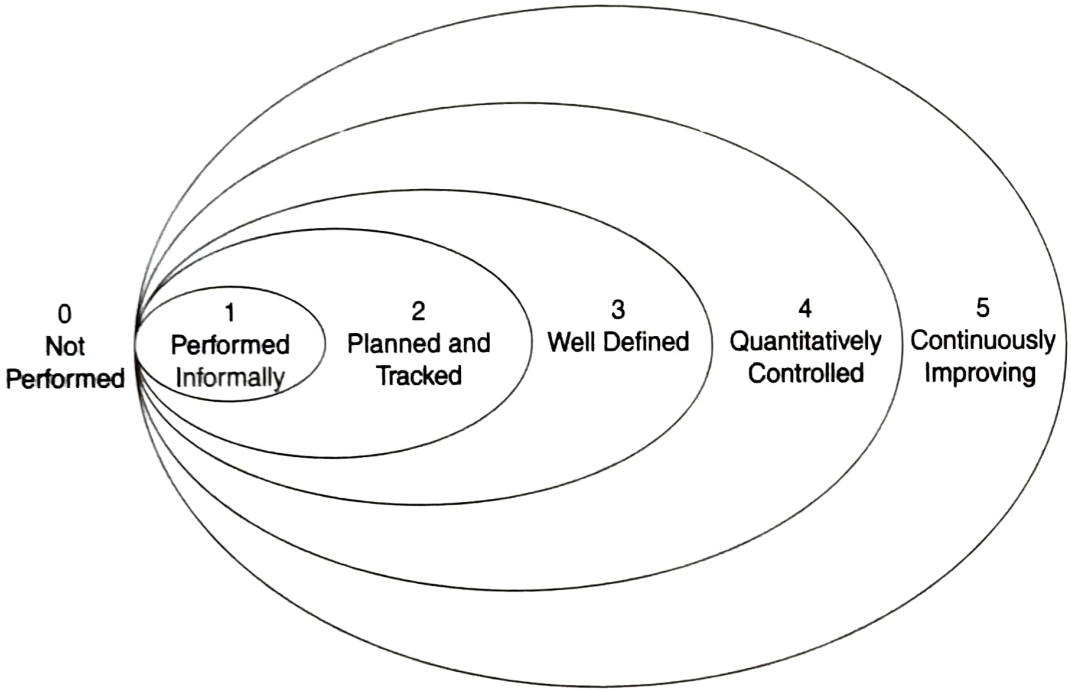


Figure 4.2 Capability levels for maturity of security engineering practices.
Courtesy: Systems Security Engineering Capability Maturity Model – Model Description Document Version 3.0.

Standards, Guidelines and Procedures

Recall that Figures 4.1 and 4.5 (on page 65) represent the hierarchical nature of relationship between *business goals* and *objectives*, *technology strategy*, *information security strategy*, *standards* and *procedures*. Figure 4.3 presents the components/building blocks of information security. The word 'policy' is prominent in all these figures and therefore we must now discuss some most common terms in connection with security management, namely *policies*, *standards*, *guidelines* and *procedures*.

In reference to Figures 4.1 and 4.5, it can be seen that the next level down from policies consists of the three elements of policy implementation, namely *standards*, *guidelines* and *procedures*. These three elements hold the actual details of the policy, such as how it should be implemented and what standards and procedures should

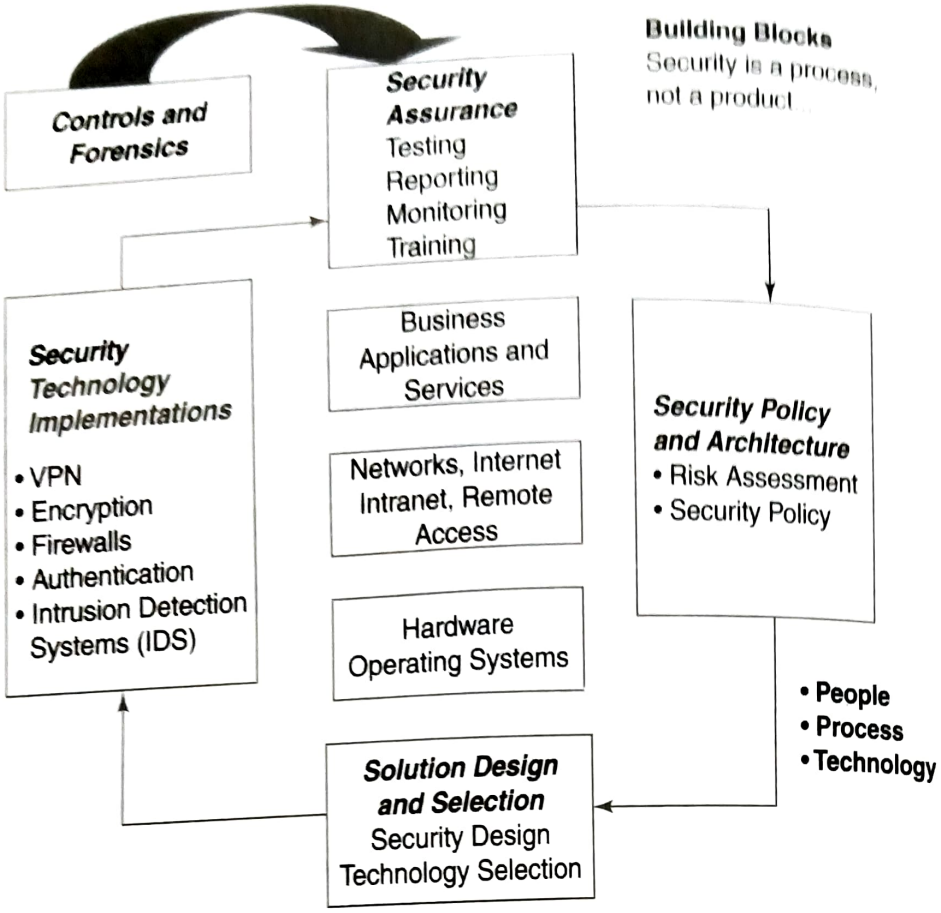


Figure 4.3 | Building blocks of information security.

be followed. They are published in an organization via manuals stored on the company intranet, booklets for distribution to the employees and other entities concerned with it, for spreading security awareness in the organization. An important point to note is that standards, guidelines and procedures are separate yet linked documents from the general policies, especially the senior-level policy statement. It is not a recommended practice to create a single document to cover the needs of all these elements. Some examples for the policies mentioned above are provided in Boxes 4.3 and 4.4.

Box 4.3 Electronic Mail (E-Mail) Policy: An Example

In an organization, the following may be stipulated with respect to the use of e-mails by employees and individuals who work in the organization (say contractor personnel):

1. **E-Mail policy coverage:**
   - Confidentiality of information disclosed through e-mail communication;
   - sender's responsibility for the contents of the e-mails;
   - disclosure of sensitive information such as passwords, personal identification number (PIN) and credit card.
2. **Appropriate use of e-mails:** Employees and other personnel working for the organization and using the organization e-mail facilities shall use e-mail strictly for business use only.
   - No obscene or profane message should be sent through e-mails.
   - E-Mail should not be used for sending spam mails, chain mails, graphics, etc.

Box 4.3 *Continued...*

- E-Mails should not be automatically forwarded to addresses outside the company.
- Size of the e-mail should be restricted within approved limits set by the organization.

3. **Management's authority on e-mails:**
   - The management reserves the rights to monitor the use of e-mails.
   - The management could store the e-mails for retrieval at a later date for any legal purpose.
   - Any encryption done to e-mail attachments should be with the company's approval and the encryption key should be stored for retrieval when necessary.
4. **Disclaimer notice:** Since an e-mail is not a secure medium and it is very easy to read, copy or alter an e-mail, put a disclaimer similar to the one given as follows (the company can at least protect itself from any misuse):
   'The information in this mail is confidential and is intended solely for the addressee. Access to this mail by anyone else is unauthorized. Any copying or further distribution beyond the original recipient is not intended and may be unlawful. The opinion expressed in this mail is that of the sender and does not necessarily reflect that of the XXX company'.

Box 4.4 Password Policy: An Example

The policy on passwords can be used to define attributes with which the password must comply. The password policy, for example, can enforce the following conditions:

1. whether the user identity (ID) and password can match;
2. maximum occurrence of consecutive characters;
3. maximum instances of any character;
4. maximum lifetime of the passwords;
5. minimum number of alphabetic characters;
6. minimum number of numeric characters;
7. minimum length of the password;
8. whether the user's previous password can be reused.

4.3 Information Security Scenario in the Financial Sector

In the financial sector, the Reserve Bank of India (RBI) has created a comprehensive document that lays down a number of security-related guidelines and strategies for banks to follow in order to offer Internet banking. The guidelines broadly talk about the types of risks associated with Internet banking, the technology and security standards, legal issues involved and regulatory and supervisory concerns. Any bank that wants to offer Internet banking must follow these guidelines and adhere to them as a legal necessity.

Recent InfoSec surveys indicate that the banking and finance sector companies, most serious about security, are the major investors in security solutions, and regularly revise their security policies following periodic audits. Next in line are the software service companies, business process outsourcing (BPO) firms and IT-enabled services companies. However, verticals such as manufacturing continue to lag, except the companies that have extensive enterprise resource planning (ERP) setups or those that drive their supply chain through the web. Aside from these three verticals, companies in other verticals have a long way to go in establishing InfoSec.

4.4 Information Security Management System (ISMS)

In the preceding sections, we discussed the working of security-related practices through policies, standards and procedures. A mechanism that works well for this is an *ISMS*, whose objective is to provide a systematic approach to managing sensitive information in order to protect it. It encompasses employees, processes and information. An ISMS is depicted in Figure 4.4. We can see that some basic measures must be applied to secure the information system. Security threats must be managed and controlled; establishing a global policy, that is, a broad security policy, with management involvement helps to do this. While doing this, four levels of documentation emerge, as depicted in Figure 4.4.

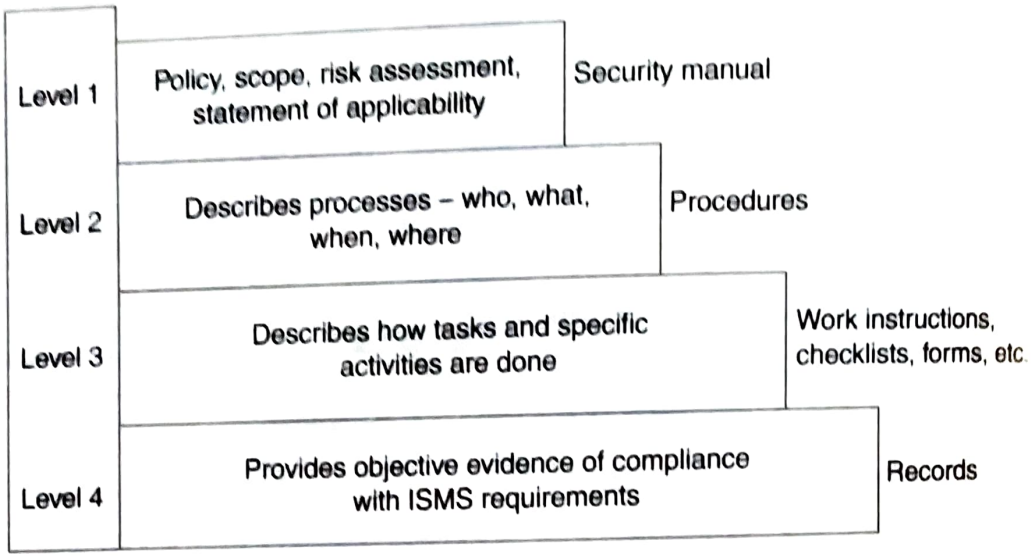


Figure 4.4 | Documentation levels in information security management system.

In the previous chapter, we discussed threats to information systems (IS). In this chapter, in the earlier sections, the discussion was on the management's role for security formation. Given that it is necessary for the organizations to identify the nature of possible threats to its IS, one of the best practices is to establish a set of measures, called 'controls'. Controls are meant to ensure the security of IS and, beyond that, to also ensure the privacy and confidentiality of information stored in the systems. It is then necessary to continually evaluate the controls with the auditing process. A detailed discussion on this is available in Chapter 35 devoted to security audits. We end this section by providing two mini cases as an exercise in Box 4.5.

Box 4.5 Mini Cases

Mini Case 1

Company *XYZ* is a small company (20 people) with a manager and a system administrator reporting to him/her. The two prepare a security policy, according to which some operations will have to be authorized by the manager and executed by the system administrator, and the manager will know all the passwords and commands needed and how to access and modify the logs. What is wrong in this situation? What rule has been violated?

Mini Case 2

Company ABC is a part of an organization based in the United States. The company in the United States, as part of a recent decision to create a presence outside the United States, has bought the control of small companies based in India, Singapore, Taiwan and Malaysia. A part of the process for integrating the various parts is to create a committee that includes a

Box 4.5 *Continued...*

member of their legal department (to verify the legal compliance). The company then plans to send managers from their headquarters (based in the United States) to each country to make sure the policy is implemented correctly. What is wrong in this planning?

4.5 Organizational Responsibility for Information Security Management

We discussed security policies, standards, guidelines, etc. (refer Figure 4.1). Ideally, 'best practices' begin at the top and percolate down in the organization. The senior management team members of an organization are the 'strategists' with 'vision' and long-term view. They exemplify their asset protection intent with the well-set policies directed toward this.

However, often, as it happens, too small a budget, too few personnel and too little consciousness of the management constitute approximately half of the obstacles for IT security according to a study of the META Group (see Figure 4.6). It may also happen that the IT budgets invested in IT security go wrong in the long term. Given this, one of the important tasks for the top management in an organization is to make their employees aware of the IT security significance. This starts with the formation of 'security policies' as we see in this chapter. Security *policies*, *standards* and *procedures* stand in a certain hierarchical relationship in alliance with the organization's overall business goals. This is illustrated in Figure 4.5. There are a few important points to be noted with respect to Figure 4.5. First of all, to be understood and effective, InfoSec policies

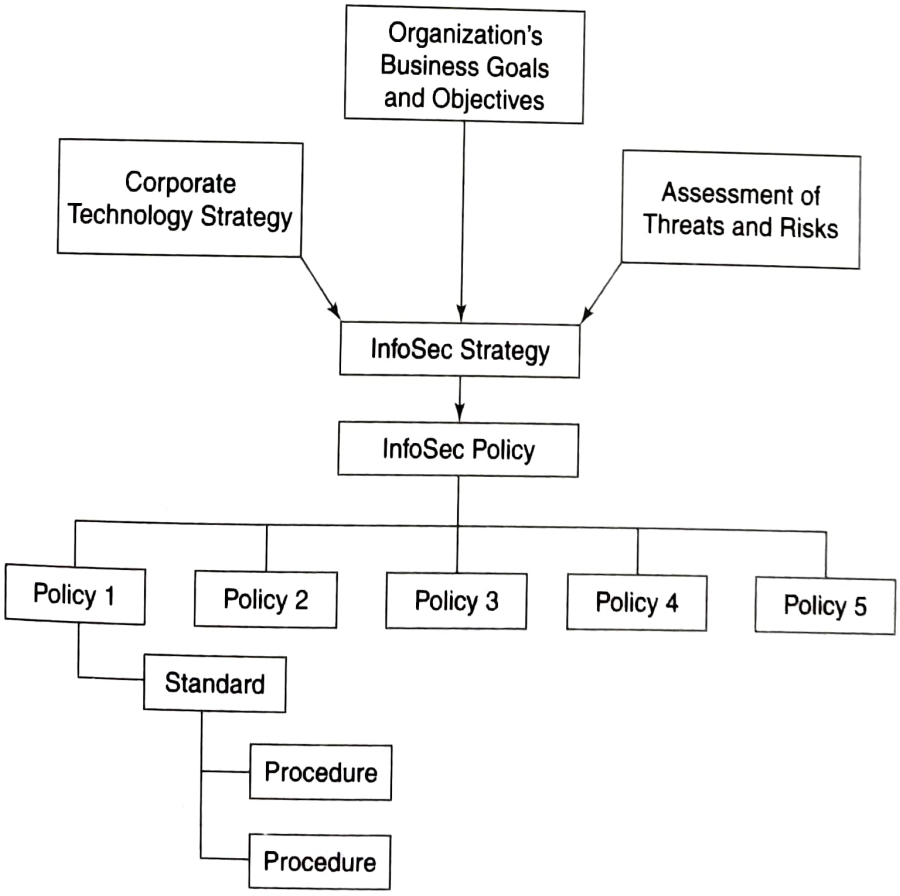


Figure 4.5 | Hierarchy of security policies, standards and procedures.

must be traceable back to the corporate objectives. This is of foremost importance. As an example of business goals/objectives, consider the following broad statement: 'We shall embrace and expand the use of electronic commerce (e-commerce) and related technologies in order to achieve cost reduction and business efficiency to serve our world-wide customers' A company might state: 'We will increase the reach of our core business applications to our customers through the use the Internet and the World Wide Web'. This is an example of corporate technology strategy mentioned in Figure 4.5. Typically, the management works together with the Chief Security Officer (CSO) and Chief Information Officer (CIO) taking their technical assistance to find the most possible way a hacker or virus will take to get into the system. So, after performing a scan of its business operations environment, an organization may arrive at a conclusion that they operate at a high level of risk in its protection of sensitive information assets. This could be the result of having performed an assessment of the threats and the resulting risks as mentioned in Figure 4.5. To counter this, an organization may form a strategy saying: 'We will use cost-effective security measures to protect our information assets.' A statement for the overall security policy of an organization might read like: 'All users will be authenticated whether or not working remotely. This will be applicable to full time employees in permanent service of the organization as well as those sourced from contractors.' A 'standard' could be: 'Remote access users will use dual-factor authentication using (so-and-so) authentication tokens.' Finally, the specific security procedure corresponding to a chosen standard could be: 'Users are to contact the remote access security administrator to receive their authentication token after they have been approved for such access'.

Thus, we can see that the management role lies in defining business strategies, guidelines and processes/procedures as well as considering the volume of data, systems, subprocesses and persons. This is endorsed by the SSE-CMM wherein the following is the generic practices list under the common feature of 'planning performance':

1. allocate *resources*;
2. assign *responsibilities*;
3. document the *process*;
4. provide *tools*;
5. ensure *training*;
6. plan *the process*.

Hence, the management in an organization should erect an IT standard and security structure that is magisterial for all the employees. It is thus important that the management deals with the topic of IT security and does not simply delegate it to the IT departments. A central user administration is necessary in order to get a whole functional security system without the need for a high budget. But technical solutions alone are not sufficient in order to guarantee an extensive security. In addition to organizational methods, employee sensitization to security awareness is of great importance. Security does not represent a product that can be installed uniquely, it is an ongoing process.

Box 4.6 Industry Leaders' Thoughts on InfoSec

1. 'Information Security is a combination of various factors. It involves technology, people and policy.'– Sameer Kapoor, Executive Director, PricewaterhouseCoopers Pvt. Ltd.
2. 'Information Security is not just a technology issue – this is a people and process issue too. The answer to this is education and awareness. You should talk to your employees.' – Capt. Raghu Raman, Practice Head, Special Services Group, Mahindra Consulting.
3. 'Security has to move away from being a technology issue and become a business related issue.' – Sunil Chandiramani, Partner, Ernest & Young.

Courtesy: The above views are quoted from a public domain website (Network Magazine issue of April 2003)

4.6 Information Security Awareness Scenario in Indian Organizations

Majority of the Indian software businesses are driven by multinationals located mainly in the United States. Today, the US InfoSec industry stands over USD 8.7 billion [see the uniform resource locator (URL) quoted in the *Further Reading* section]. In the present global digital economy, information flows more often than not through the complex IT infrastructure present. To be efficient at managing, operating and protecting this IT infrastructure, there is a need for having a common set of guidelines for the use and access of information assets. Therefore, we discussed policies, guidelines and standards for information systems security.

In the global context for IS and the threats to IS (Chapters 1 and 2), it is clear that many business processes do not work without reliable IT systems' confidentiality, and thus, *integrity* and *availability* of information are of high importance in today's business life. So, let us understand where do we stand on 'IT/information security awareness' as far as the Indian scenario is concerned.

The complexity of security administration in managing large networks is, nowadays, a big issue. Although organizations know about the ever more frequent security attacks, they update their safety devices only when it is already too late. This can only be ascribed to 'attitude' and 'mindset' problems with respect to security. Although the scenario is progressively improving, awareness of Indian companies in the matter of information systems security still is far behind that of European countries and the United States. Figures 4.6 and 4.7 show the status on 'security awareness' and 'security challenges' faced by most Indian organizations. Although it is based on some past surveys, it is illustrated here only to drive home the point that heightening this awareness is important because India, among other countries in the South East Asian region, is now becoming one of the preferred off-shore locations (mainly owing to cost reasons and availability of English-speaking IT-trained manpower) for outsourcing businesses.

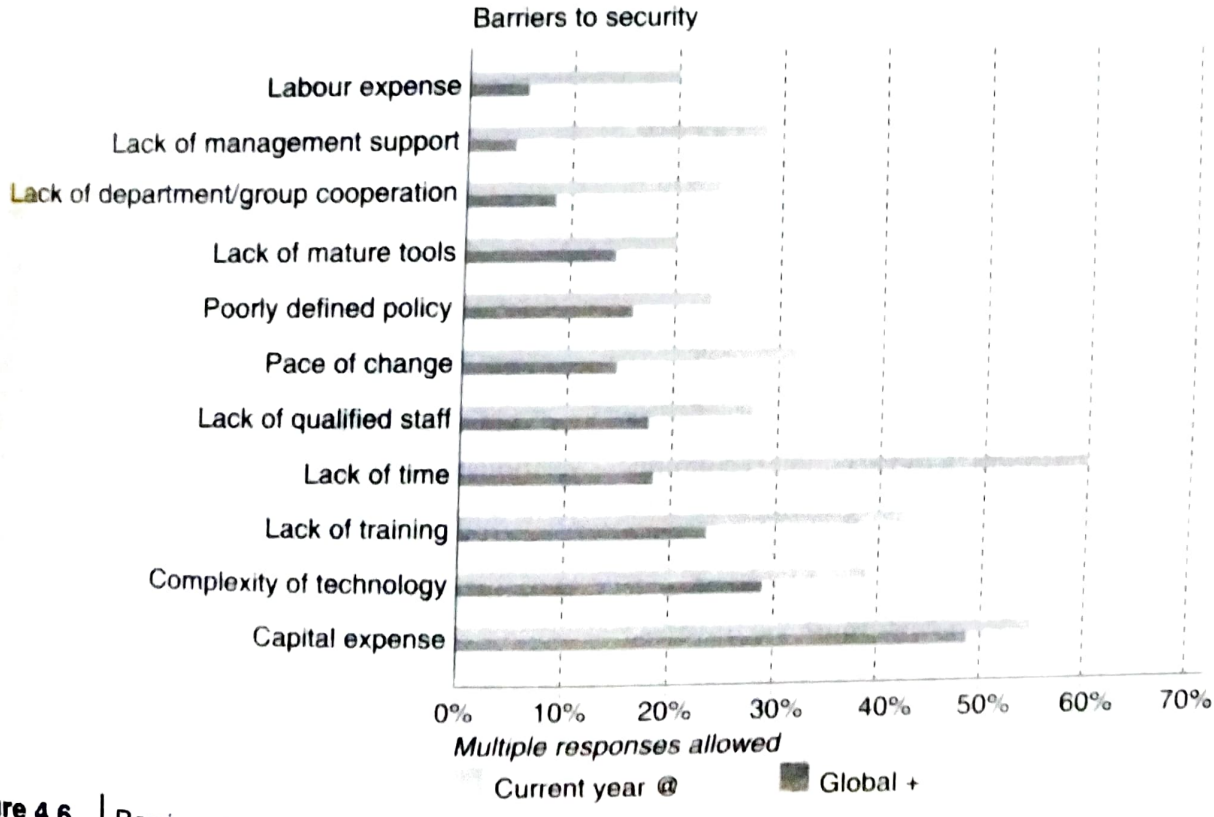


Figure 4.6 | Barriers to security.

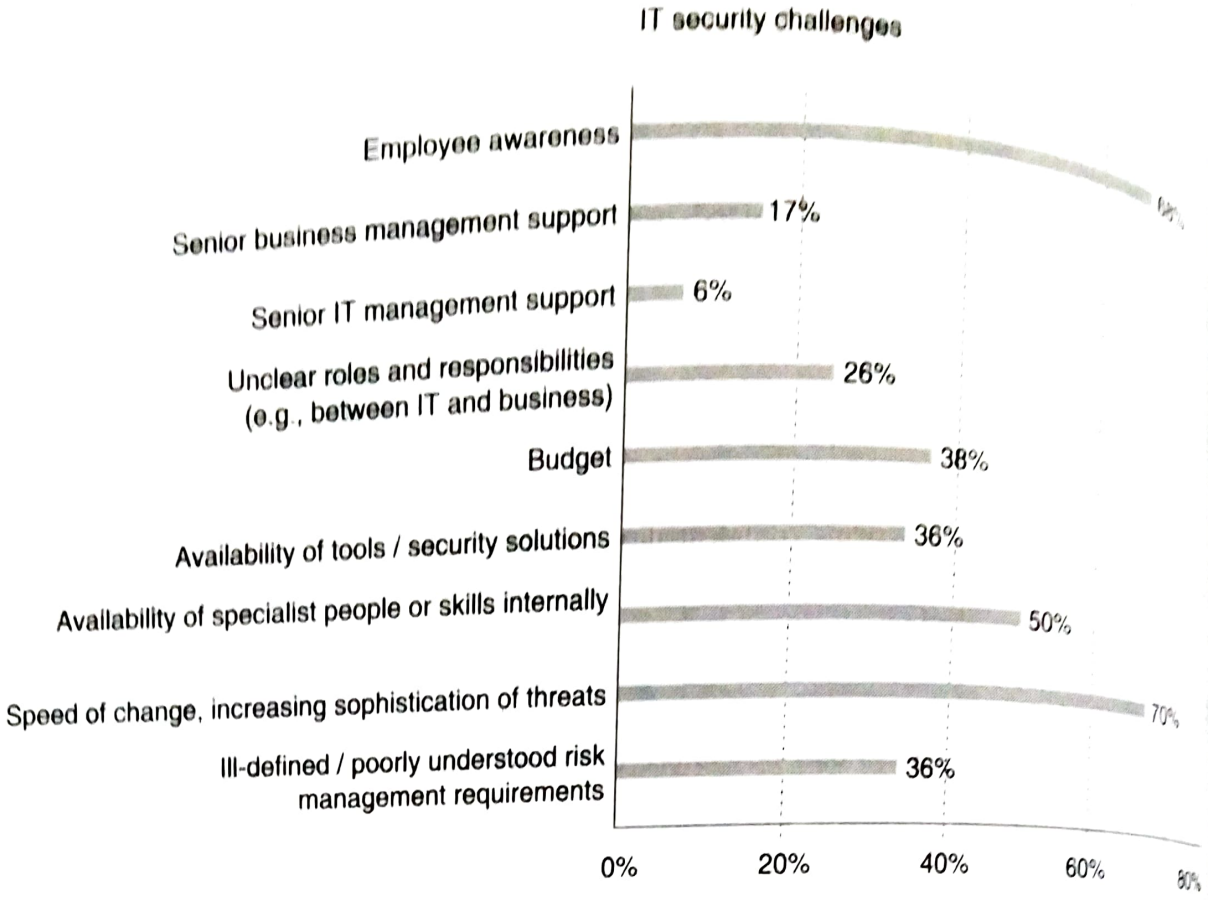


Figure 4.7 | IT security challenges for Indian organizations.

Owing to factors such as globalization and reasons of regulatory nature, certain Indian companies are now more serious about information security. But the rest are complacent and need to do a lot more than just implementing solutions. International companies, seeking to outsource work to Indian firms, insist on security assurance/security certification and security governance. They insist on adherence to laws, standards and business practices prevalent in their respective countries. Not surprisingly, the top software services companies, IT-enabled services companies and BPO outfits are going in for security certifications such as BS 7799 or ISO 17799. Thus, regulatory requirements become one more driver for increased security awareness.

Summary

IS in an organization will continue to face threats given the global paradigm in today's digital economy. It is the responsibility of the management to address the security issues by forming appropriate security policy. The matter of security implementation is complex and all stakeholders must be involved to understand and commit to the hierarchical relationship of the organization's business objectives to its security policies down to procedures. Standards and guidelines must also be considered for their role in security policy.

Review Questions

4.1 Explain the role of senior management in an organization with respect to information security management.

4.2 Explain the hierarchical relationship between policies, standards, guidelines and business

5 Building Blocks of Information Security

Learning Objectives

After completing this chapter you will be able to:

- understand basic concepts that are the building blocks for InfoSec.
- learn InfoSec related basic definitions.
- understand the three pillars of information security.
- understand information classification and the criteria for classification and learn to categorize business systems.
- learn about various roles involved in information classification (this will help in appreciating concepts in asset management re-emphasized in Chapter 37).
- understand data obfuscation.

5.1 Introduction

So far, we have discussed about the role of information systems (IS) in the global context, the crucial role that IS play in the modern digital economy, how information systems are getting complex given the combined effect of globalization and liberalization, etc. (Chapter 1). In Chapter 2, we discussed how the developments in information technology (IT) open door to new threats, typical attacks on computer-based IS, how various threats are classified, etc. Chapter 3 was devoted to the new phenomenon called mobile computing and the unique threats that come in due to proliferation of handheld devices and the impending security implications for organizations in this new paradigm of mobile workforce. In Chapter 4 we had the important discussion on organizational scenarios in information systems security. We discussed about organizational responsibility for the information systems security. We also explained the role of security policies and security procedures, standards and guidelines, etc. With this background, we now present the layers of information security (InfoSec).

5.2 Basic Principles of Information Systems Security

With the background set through earlier chapters, our aim in the current chapter is to provide a comprehensive overview of the fundamental concepts in InfoSec. This is essential for forming the right kind of background for the discussion on risk assessment and analysis, which is the cornerstone for any security management exercise in organizations. Concepts developed here are important as the reference point for the next chapter. Before proceeding further, we present the security goals in Figure 5.1. These are also known as the 'three pillars of InfoSec'.

The ideal approach to security is the 'onion skin' approach (depicted in Figure 5.2, in which the failure of any security control will not leave an asset completely unprotected; this is the concept of 'defense-in-depth'. In Chapter 1, we had provided a discussion to understand what IS mean. Reader must understand that the term 'system' is very generic and its meaning can change with context. In the paradigm of information systems security, 'system' can denote a number of things:

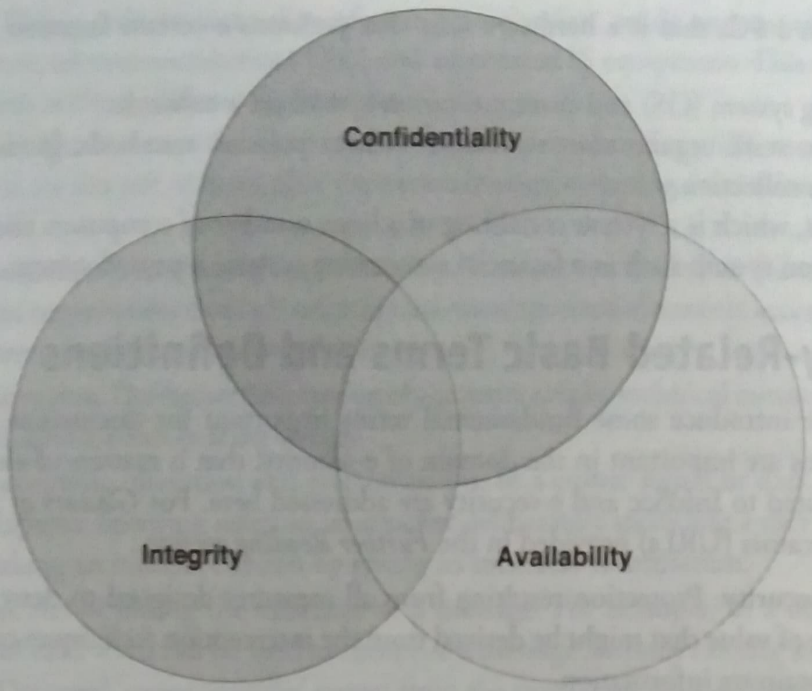


Figure 5.1 | Security goals.

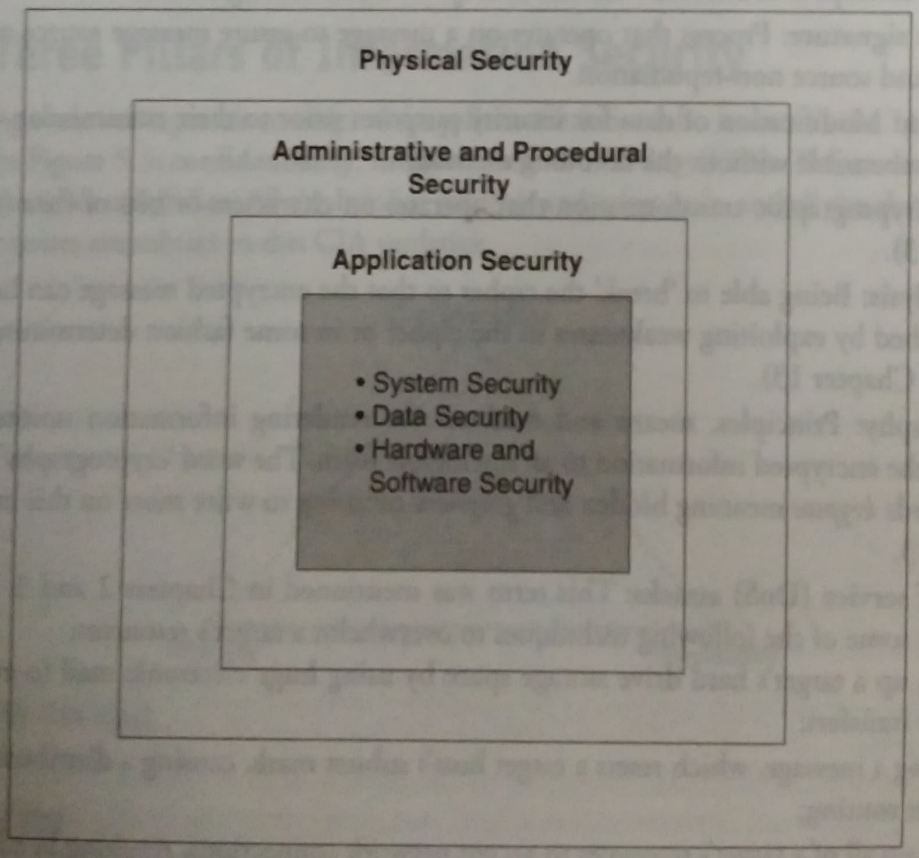


Figure 5.2 | Security layers.

1. A product or component, for example, a protocol for cryptograph, a card for wireless network access, a smart card or say a motherboard or Personal Computer Memory Card Industry Association (PCMCIA) card (see the URL in the *Further Reading* section) of a personal computer (PC), disk

controller on a PC, that is a hardware unit that performs a certain function with the virtue of its design.

2. An operating system (OS) and communication system on a network.
3. Organization staff, organization structure, security policies, standards, guidelines and procedures together as a collection.
4. The Internet, which is a system consisting of a large number of computers and computer networks.
5. An application system such as a financial accounting system, a payroll system, etc.

5.3 Security-Related Basic Terms and Definitions

In this section, we introduce some fundamental terms important for discussions about security-related topics. These terms are important in the domain of e-security, that is matters of electronic security. Only the major terms related to InfoSec and e-security are addressed here. For *Glossary of Security Terms* visit the uniform resource locators (URLs) provided in the *Further Reading* section.

1. **Electronic security**: Protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the interception techniques or any other illegitimate means of obtaining information.
2. **Non-repudiation**: Method by which the sender of data is provided with a proof of delivery and the recipient is assured of the sender's identity (ID), so that neither can later deny having processed the data. This concept is connected with the concept of 'electronic signature'.
3. **Electronic signature**: Process that operates on a message to assure message source authenticity and integrity, and source non-repudiation.
4. **Encryption**: Modification of data for security purposes prior to their transmission so that they are not comprehensible without the decoding method.
5. **Cipher**: Cryptographic transformation that operates on characters or bits of data (more on this in Chapter 13).
6. **Cryptanalysis**: Being able to 'break' the cipher so that the encrypted message can be read. It can be accomplished by exploiting weaknesses in the cipher or in some fashion determining the key (more on this in Chapter 13).
7. **Cryptography**: Principles, means and methods for rendering information unintelligible and for restoring the encrypted information to an intelligible form. The word 'cryptography' comes from the Greek words *kryptos* meaning hidden and *graphein* meaning to write more on this in Section 13.2 of Chapter 13.
8. **Denial of service (DoS) attacks**: This term was mentioned in Chapters 2 and 3. The DoS attack might use some of the following techniques to overwhelm a target's resources:
   - filling up a target's hard drive storage space by using huge electronic mail (e-mail) attachments or file transfers;
   - sending a message, which resets a target host's subnet mask, causing a distribution of the target's subnet routing;
   - using up all of a target's resources to accept network connections, resulting in additional network connections being denied.

   Subnet mask is a scheme that distinguishes network ID from host ID. It is used to specify whether the 'destination host' is *local* or *remote*. For understanding the basics of subnet mask, readers are encouraged to visit the URLs provided in the *Further Reading* section.
9. **Interception**: This term is typically used with defense systems and warfare. The term is introduced here because it is used in explaining other security-related terms in this section.

10. **TEMPEST**: This is a short name that refers to investigation, study and control of compromising emanations from telecommunications (TC) and automated IS equipment. This term is often used in connection with military/defense applications.
11. **TEMPEST test**: This is yet another term used in connection with military/defense applications. It refers to laboratory or on-site test to determine the nature of compromising emanations associated with TC or automated IS.
12. **TC and automated information systems security**: Protection afforded to TC and automated IS, in order to prevent exploitation through interception, unauthorized electronic access or related technical intelligence threats and to ensure authenticity.
13. **Technical penetration**: Deliberate penetration of a security area by technical means to gain unauthorized interception of information-bearing energy.
14. **Spoofing**: Interception, alteration and retransmission of a cipher signal or data, in such a way as to mislead the recipient. Spoofing refers to an attacker deliberately including a user (subject) or a device (object) into taking an incorrect action by giving its incorrect information.
15. **Steganography**: Art of hiding the existence of a message. For example, in a digital image the least significant bit of each word can be used to comprise a message without causing any significant change in the image. The word 'steganography' comes from the two Greek words: *steganos* meaning 'covered' and *graphein* meaning 'to write'. Steganography can be used to make a digital watermark to detect the illegal copying of digital images. Thus, it aids confidentiality and integrity of the data.

5.4 The Three Pillars of Information Security

The following three concepts are considered the pillars of InfoSec (also known as the 'big three' in InfoSec, as shown in Figure 5.3: **confidentiality**, **integrity**, and **availability** (CIA). These concepts represent the fundamental principles of InfoSec. All the InfoSec controls and safeguards, and all the threats, vulnerabilities and security processes are subject to this CIA yardstick.

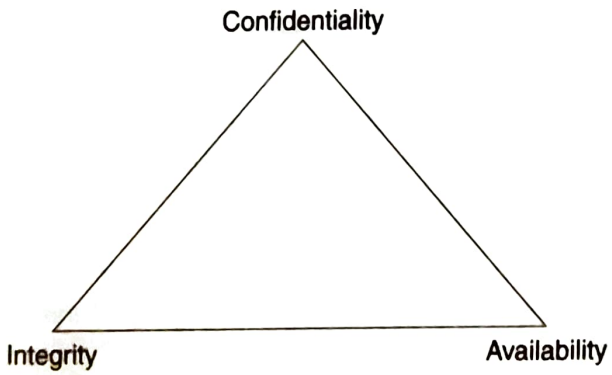


Figure 5.3 | The CIA triad.

Confidentiality

In the domain of InfoSec, the concept of 'confidentiality' is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways, such as through the intentional release of private company information or through a misapplication of network rights. Similar issues (loss of confidentiality) in mobile computing were discussed in Chapter 3.

Integrity

This is yet another very important concept in InfoSec. The concept of integrity ensures that

1. Modifications are not made to data by unauthorized personnel or processes.
2. Unauthorized modifications are not made to data by authorized personnel or processes.
3. The data are internally and externally consistent, that is the internal information is consistent among all subentities and the internal information is consistent with the real world, external situation (Box 5.1 along with the included figure illustrates an example of data integrity).

Box 5.1 What Loss to Data Integrity and Confidentiality Means to Organizations

It is important that data adhere to a predefined set of rules, as determined by the database administrator (DBA) or application developer. As an example of data integrity, consider the simple data as in a payroll application or employee master data. Tables are called employees and departments and present the *business rules* for the information in each of the tables, as illustrated in the figure on the next page (note that some columns in each table have specific rules that constrain the data contained within them):

This illustration shows tables called DEPT and EMP. Table DEPT has three columns:

1. DEPTNO;
2. DNAME;
3. LOC.

Each value in the DNAME column must be unique. Table EMP has six columns:

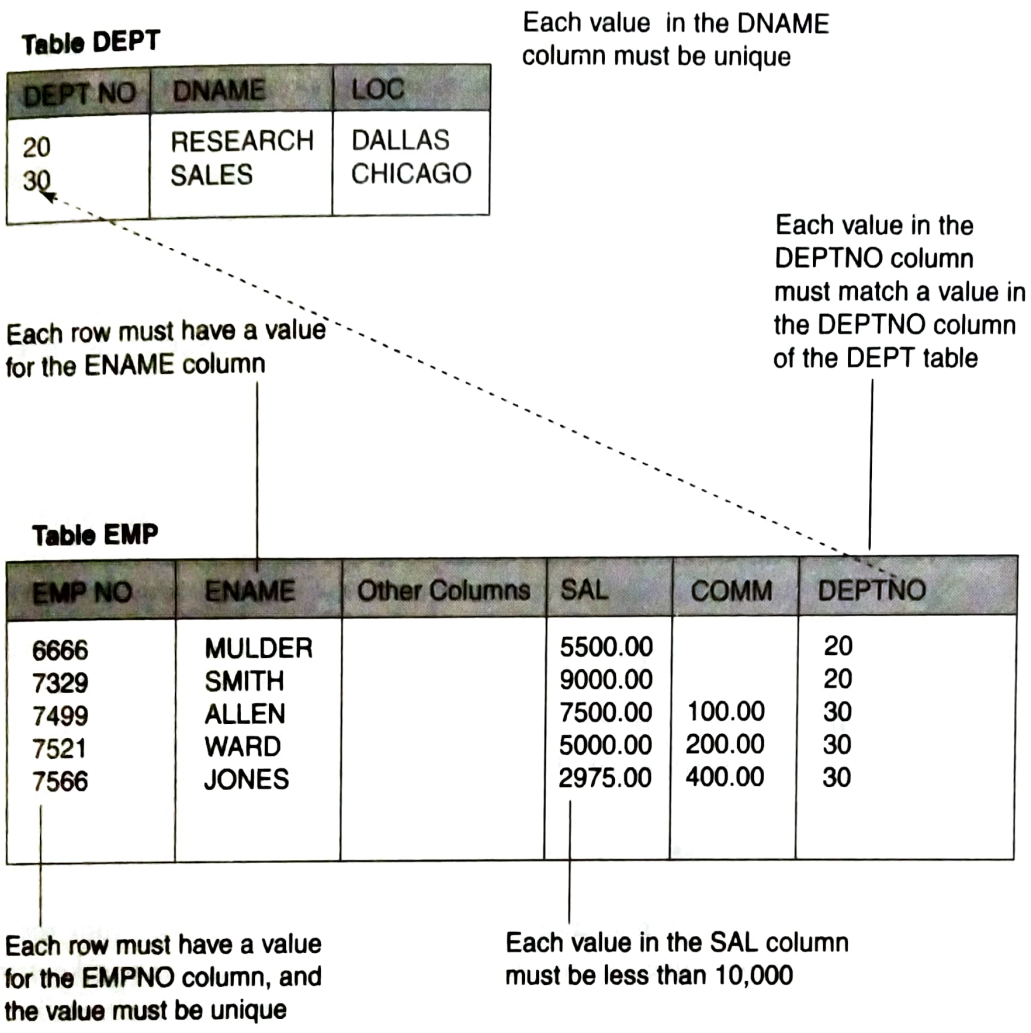
1. EMPNO;
2. ENAME;
3. Other columns;
4. SAL;
5. COMM;
6. DEPTNO.

Each row must have a value for the ENAME column. Each row must have a value for the EMPNO column, and the value must be unique. Each value in the DEPTNO column must match a value in the DEPTNO column of the DEPT table. Each value in the SAL column must be lower than 10,000.

In addition to the above, there are many other examples of loss of data confidentiality and data integrity. For example, through erroneous action, IT users can allow or cause loss of data confidentiality/integrity. The consequential damage depends on the sensitivity of the data involved. Examples of such erroneous actions are:

1. Through oversight, printouts containing personal data are not fetched by staff members from the network printer.
2. Floppy disks are dispatched without prior physical deletion of previously stored data.
3. Owing to incorrectly administered access rights, a staff member can modify data.
4. Unable to assess the critical impact of such a violation of integrity.
5. New software is tested using non-anonymous data. Unauthorized employees thus gain access to protected files or confidential information. It is also possible that third parties also become aware of this information as the disposal of 'test printouts' is not correctly handled.

Box 5.1 *Continued...*



Availability

This is the last of the important triad in InfoSec. The concept of 'availability' ensures the reliable and timely access to data or computing resources by the appropriate personnel. In other words, 'availability' guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.

In the light of the illustration in Box 5.1, it is important to note that DAD is the reverse of CIA. DAD is **disclosure** (opposite of confidentiality), **alteration** (opposite of integrity) and **destruction** (opposite of availability) of information.

5.5 Other Important Terms in Information Security

The term automated information systems security is synonymous with computer security. There are also several other important concepts and terms that a security professional/security practitioner/students of InfoSec course must fully understand. These concepts include **identification, authentication, accountability, authorization** and **privacy**. Let us have a brief description of each of these terms:

1. **Identification**: It indicates the means by which users claim their identities to a system. It is commonly used for access control, and is necessary for authentication and authorization.
2. **Authentication**: This is the testing or reconciliation of evidence of a user's ID. It establishes the user's ID and ensures that the users are who they say they are. Authentication is a security measure designed to establish the validity of a transmission, message or originator, or a means of verifying an individual's eligibility to receive specific categories of information.
3. **Accountability**: A system's ability to determine the actions and behavior of a single individual within a system, and to identify that particular individual. Audit trails and logs support accountability.
4. **Authorization**: The rights and permissions granted to an individual (or process), which enable access to a computer resource. Once a user's ID and authentication are established, authorization levels determine the extent of system rights that an operator can hold. Thus, authorization is the actual rights granted to a user, program or process.
5. **Privacy**: This means the level of confidentiality and privacy protection that a user is given in a system. It is an important component of security controls. Privacy guarantees not only the fundamental tenet of confidentiality of a company's data, but also the privacy level of data, which is being used by the operator. For detailed discussion on privacy concepts refer Chapter 29.

5.6 Information Classification

Having discussed some basic security terms, we now turn to another important topic from security perspective: information classification. Generally speaking, organizations like to classify their information for suitable treatment in terms of InfoSec. It is not possible to protect all the information and IS in the organizations. There are several reasons why the organizations (government, private, public and defense) like to classify information. The main reason is that not all data/information have the same level of importance or same level of relevance/criticality to an organization. From the discussions in Chapters 1 and 2, one can see that some data are more valuable to the people who make strategic decisions (senior management) because they aid them in making long-range or short-range business direction decisions. Some data, such as trade secrets, formulae (used by scientific and/or research organizations) and new product information (such as the one used by the marketing staff and sales force), are so valuable that their loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility. Events like those could damage the company's goodwill.

Thus, it is obvious that information classification provides a higher, enterprise-level benefit. In Chapter 1, we discussed IS in a global context indicating that the information can have an impact on a business globally, not just on the business unit or line operation levels. The primary purpose is to enhance CIA, and to minimize the risks to the information. It is well known that in most countries, information classification has had the longest history in the government sector. Its value has been established, and it is a required component when securing trusted systems. In this sector, information classification is primarily used to prevent the unauthorized disclosure and the resultant failure of confidentiality.

The other reason for information classification may also be the compliance required with privacy laws and legislations, or other regulatory compliance. A company may wish to employ classification to maintain a competitive edge in a tough marketplace. There may also be sound legal reasons for a company to employ information classification, such as to minimize liability or to protect valuable business information. In all, classification of information and information assets helps organizations to apply security policies and security procedures toward protection of information assets that are considered critical. We can summarize the benefits of information classification as follows:

1. Information classification is a demonstration toward an organization's commitment to security protections.
2. It helps identify which information is most sensitive or vital to an organization.
3. It supports the tenets of CIA as it pertains to data (the pillars of InfoSec discussed in earlier part of this chapter).
4. It helps identify which protections apply to which information.
5. It fulfils statutory requirements toward regulatory, compliance or legal mandates.

Thus, the key point is that the information produced or processed by an organization must be classified according to the organization's sensitivity to its loss or disclosure. These data owners are responsible for defining the sensitivity level of the data. This approach enables the security controls to be properly implemented according to its classification scheme. In the next section, terms used for classification of data/information are introduced.

5.7 Terms for Information Classification

The following definitions describe several schemes used for levels of data/information classification, ranging from the lowest to the highest level of sensitivity:

1. **Unclassified**: Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.
2. **Sensitive but unclassified** (SBU): Information that has been designated as a minor secret, but may not create serious damage if disclosed. Answers to tests are an example of this kind of information. For example, consider health care information of a hospital.
3. **Confidential**: Information that is designated to be of a confidential nature. The unauthorized disclosure of this information could cause some damage to the country's national security. This level is used for documents labeled between SBU and secret in sensitivity.
4. **Secret**: Information that is designated to be of a secret nature. The unauthorized disclosure of this information could cause serious damage to the country's national security.
5. **Top secret**: This is the highest level of information classification (e.g., information in defense organizations). Any unauthorized disclosure of top secret information will cause exceptionally grave damage to the country's national security.

Given the 'information overload' in the present dynamic business environments, it is neither good to deal with too much information nor good to provide employees and other business entities with 'all' the data. Therefore, the organizations make data available to those concerned on a 'need-to-know' basis. For this reason, the following data/information classification is also prevalent in most private organizations:

1. **Public**: Information that is similar to unclassified information (see above), that is all of an organization's information that does not fit into any of the other categories can be considered public. This information should probably not be disclosed. However, if it is disclosed, it is not expected to seriously or adversely impact the company.
2. **Sensitive**: Information that requires a higher level of classification than normal data. This information is protected from a loss of confidentiality, as well as from a loss of integrity owing to an unauthorized alteration.
3. **Private**: Typically, this is the information that is considered of a personal nature and is intended for company use only. Its disclosure could adversely affect the company or its employees. Salary levels and medical information could be considered as examples of 'private information'.

5.8 Criteria for Classification of Data and Information

In view of the discussion so far and Box 5.2 illustrating data integrity issues, let us now discuss the criteria could be used for classifying information that is treated as a corporate resource. Several of the following criteria are used to determine the classification of an information object:

1. **Value**: It is the most commonly used criteria for classifying data in the private sector. If the information is valuable to an organization or its competitors, it needs to be classified.
2. **Age**: The classification of the information may be lowered if the information's value decreases over time. In the Department of Defense, some classified documents are automatically declassified after a predetermined time period has passed.
3. **Useful life**: If the information has been made obsolete owing to new information, substantial changes in the company or other reasons, the information can often be declassified (considerations like these are especially important in CRM, data warehousing and DM domain).
4. **Personal association**: If information is personally associated with specific individuals or is addressed by a privacy law, it may need to be classified. For example, investigative information that would reveal informant names may need to remain classified.

Box 5.2 Data Integrity and Availability Issues in CRM Environment

CRM stands for *customer relationship management* (Parvatyar, Sheth & Shainesh, 2005; Gosine & Boehm, 2000; Brown, 1999). CRM applications are dependent on good quality transactions data that can be captured into a company's *data marts* that, in turn, can be used for the purpose of data *mining* (DM). CRM along with DM is used for making a number of strategic decisions for the business.

Despite the proliferation of enterprise resource planning (ERP) systems and other integrated technologies, many organizations store their related data in several disconnected systems, each of which is available to a limited number of people within specific departments. For example, an accounting system contains customer records, transactions and payment histories. Prospect or contact records may exist in a contact management system, or Outlook. Correspondence may exist within saved Word documents on a server and e-mails are scattered across any number of desktops in different departments.

Marketing campaign results and quarterly revenue forecasts may populate a series of spreadsheets. Other information may reside on the laptops of individual consultants or field workers, where the information is unavailable to many who may have a periodic need for it. Some of the information in these disparate sources is of the same type (client contact information) and much of it is different, yet it is all related to the work of the organization and its clientele. These 'islands of data' often create several disadvantages for the organization that operates in this environment, but many of the disadvantages can be overcome by the broader features of a CRM solution.

For the discussion on basic InfoSec concepts in this chapter, it is important to understand the operational problems posed for an organization in the light of what is said above. This is explained as follows:

1. **System management issues:** The more applications and databases that a company has running, the more potential 'points of failure' there are in the information environment. The workload of any IT department increases with the number of applications and databases that it supports. It is a known fact that it is easier to manage 1 software application than 10. Having information in hundreds of databases makes no sense – it is extremely difficult to extract information out of offragmented systems. Since several existing applications can be subsumed by a single data integrity solution, it is important for the organizations to streamline corporate information in an integrated database environment.

Box 5.2 *Continued...*

2. **Duplication of efforts inputting data:** Multiple systems that store some of the same information often require the data to be entered multiple times. If two or more people are entering client data into different systems, they are wasting both time and effort. Those separate systems may be replaced by a single CRM application in which client information is entered one time, and made available to all groups and departments that need it. But the problem does not stop there.
3. **Data integrity issues – same information entered differently by different individuals:** Duplicated data entry can have extensive negative impact. Users may enter the data differently, leading to different interpretations of the same information. If the data change over time, it can be difficult to know which data are current – this creates serious problems for DM applications. For example, a client's address can be stored in two separate systems. Sales person might update the information on her laptop, but the address will remain unchanged in the database at the back-end used for generating various business reports. One needs a system to consolidate these records, so that only one record needs to be maintained, and the current information becomes available to all. Therefore, the well-integrated corporate databases can help to improve the overall integrity of data within the organization for their use in CRM.
4. **No data synergy:** When your client data are stored in different places, your view of 'all that is happening' with respect to an issue is limited by the particular database with which you are working, and therefore, your ability to make optimal business decisions can be limited. Or you cannot find out what is going on in your business because the information is in too many places. This is a classic example of lack of data integrity. A single repository of information allows you to see 'the big picture', allowing decision makers to clearly identify the real issues, and make more effective strategic decisions.
5. **More time searching for information, less time acting on it!!** This is the real problem in most organizations suffering from lack of data integrity. There are frustrating problems caused by disparate data – time wasted searching for information. That information might simply be the contents of an e-mail that a coworker received from a client. The e-mail is on the coworkers' 'C' drive, and there is no access to it. Through integrated data systems, there should be a provision to centrally store that information where it can be available to anyone that needs it, freeing up time otherwise spent searching for the information, and instead, using the information to make more effective decisions to generate results.

Box 5.3 How do Organizations 'Classify' Data and Information?

There are many ways to do this. Several steps need to be taken for establishing a classification system. The following are some primary procedural steps:

1. Identify the owner/administrator/custodian for data/information that are considered important.
2. Specify the criteria of how information will be classified and labeled (see Section 5.7).
3. Classify the data by their owner, who has the responsibility for reviewing the data/information before handing it over for its storage as 'corporate resource'.
4. Specify and document any exceptions to the classification policy.
5. Specify the 'controls' that will be applied to each classification level, that is depending on its classification, who is authorized to access the data/information.
6. Specify the termination procedures for declassifying the information or for transfer of customer of the information to another entity or procedures of data purging or data obfuscation.
7. Create an enterprise awareness program about the data/information classification controls.

5.9 Information Classification: Various Roles

From the security perspective, the roles and responsibilities of all participants in the information classification program must be clearly defined. A key element of the classification scheme is the role the users, owners or custodians of the data play in regard to the data. The roles that *owner*, *custodian* and *user* play in information classification are described in the Table 5.1 along with their responsibilities. Concepts such as these are important for project leaders and project managers in software development organization even from configuration management and data management perspective, aspects that are emphasized by continuous improvement models such as the International Organization for Standardization (ISO) 9001:2000 and Software Engineering Institute's (SEI) Capability Maturity Model Integration (CMM-I) (see www.iso.com and www.sei.cmu.edu for details). The information on roles provided in the following table is also important from the legal perspective that is very important in security domain.

Table 5.1 | Roles and responsibilities of the owner, the custodian and the user

Role	Responsibilities
Owner	
An information owner may be an executive or manager of an organization. An owner is different from a custodian. The owner has the final corporate responsibility of data protection, and under the concept of due care, the owner may be liable for negligence because of the failure to protect these data. However, the actual day-to-day function of protecting the data belongs to a custodian	This person is responsible for the information asset(s) that must be protected. In particular, the responsibilities of an information owner include the following: 1. making the original decision as to what level of classification the information requires based on the business needs for the protection of the data 2. reviewing the classification assignments periodically and making alterations as the business needs change 3. delegating the responsibility of the data protection duties to the custodian
Custodian	
An information custodian is the delegated personnel	The duties of a custodian may include the following: 1. running regular backups and routinely testing the validity of the backup data 2. performing data restoration from the backups when necessary maintaining those retained records in accordance with legal 3. requirements established based on information classification policy Additional duties of the custodian may include being the administrator of the classification scheme
User	
In the information classification scheme, end-user is considered to be – an operator, responsibility of protecting the information by its owner. This role is commonly executed by IT systems employee or external party who routinely uses the	The following are a few important points about end-users in terms of their duties/responsibilities: 1. It is mandatory for users to follow the operating procedures that are defined in an organization's security policy, and they must adhere to the published guidelines for their use

Table 5.1 | *Continued...*

Role	Responsibilities
information as a part of their job. They can also be considered consumers of the data, who need daily access to the information to execute their tasks. Typically, managers and executives are also users along with the supervisory staff in an organization	2. Users must take 'due care' to preserve the information's security during their work (as outlined in the corporate information use policies) 3. They must prevent 'open view'* from occurring 4. Users must use the company's computing resources only for company purposes, and not for personal use (good organizations educate their users on this by the policies set for this and these rules are suitably displayed to maintain awareness on the part of the users)

*Open view: It refers to the act of leaving classified documents in the open where an unauthorized person can see them, thus violating the information's confidentiality. The procedures to prevent 'open view' should specify that information is to be stored in locked areas, or transported in properly sealed containers, for example. One more thing that users should do is use the paper shredders provided by their organizations to mitigate the risk of 'information scavenging' by any malicious users.

5.10 Data Obfuscation

Having discussed information classification in organizations and various roles associated with that, in this section we discuss an interesting method for protecting sensitive information. It involves protection of sensitive information with techniques other than encryption. 'Data obfuscation' is one of the solutions for data theft. It is related to data encryption (cryptography and encryption are discussed in Chapter 13). Although data encryption is a hot topic in the security domain, it is not a new subject, but has received an increasing amount of attention, largely owing to electronic commerce (e-commerce). Protecting credit card numbers, medical data and other sensitive information has become more important than ever before and on a larger scale. It is important to keep in mind that encryption refers to some method of modifying data so that they are meaningless and unreadable in their encrypted form. They also must be reasonably secure, that is they must not be easily decrypted without the proper key. Anything less than that will be referred as obfuscation. These are data that are rendered unusable by some means, but are not considered as a serious form of encryption. A question that may arise is why would you want to merely obfuscate data, rather than use a strong encryption algorithm? Let us understand this concept with an example.

A good example would be an audit report on a medical system (medical systems are known to have high privacy concerns). This report may be generated for an external auditor, and contains sensitive information (see Section 5.5). The auditor will be examining the report for information that indicates possible cases of fraud or abuse. Assume that the management has required that patient names, permanent account number (PAN) ID (an identification for an income tax payer) and other personal information (PI) should not be made available to the auditor except on an as-needed basis. The data need to be presented to the auditor, but in a way that allows the examination of all data, so that only patterns in the data may be detected. This kind of situation also arises when organizations provide their sensitive data to data mining (DM) experts. Encryption would be a poor choice under these scenarios, because the data would be rendered into American Standard Code for Information Interchange (ASCII) values outside of the range of normal ASCII characters. This would be impossible to read. A better choice might be to 'obfuscate' the data with a simple substitution cipher. While this is not considered encryption, it may be suitable for this situation. When the auditor finds a possible case of abuse, he will need the real name and PAN of the party involved. He could obtain this by calling a customer service representative at the insurance company that supplied the report, and ask for the

real information. The obfuscated data are read to the customer service representative, who then inputs it into an application that supplies the real data. The importance of using pronounceable characters becomes clear. Strong encryption would render this impossible.

To summarize, we can say that with data obfuscation (instead of encryption), it would not be very difficult to decipher the obfuscation scheme given enough data. A somewhat more effective method involves changing the text into segments and re-arranging it as well as obfuscating it. Next we discuss another technique for preventing sensitive data falling in the hands of unauthorized persons. Sample source code to explain data obfuscation can be found at www.teleport.com/~jkstill/util.

There is another way to 'hide' sensitive data: 'data sanitization'. 'Masking' is one of the most commonly used methods for data sanitization. Data sanitization is the process of disguising sensitive information in non-databases and development databases by overwriting it with realistic looking but false data of a similar type. The data in testing environments should be sanitized in order to protect valuable business information and also because there is, in most countries, a legal obligation to do so.

This technique is different from the previous example in that the clear text cannot be reconstructed from the displayed data. This is useful in situations where it is only necessary to display a portion of the data. A good case for this method is the receipts printed at gas stations (petrol pumps) and convenience stores. When a purchase is made with a credit card, the last four digits of the credit are often displayed as clear text (see the graphic), while the rest of the credit card number has been masked with a series of Xs as shown in the hypothetical receipt in the graphic. This method can also be used for reports where the person reading the report requires only a portion of the sensitive data. This method is also commonly used for the account numbers on printed transactions from ATMs.

```
Stop 'n' Shop
25/5/2006 8:53 P.M.

Veg Sandwitch   1    12.50    12.50

Super Petrol   12.5  49.50   618.75
                              ======
                              631.25

AMEX 2/02 XXXX-XXXXXX-65498
```

There are a number of data sanitization techniques:

1. NULL'ing out;
2. masking data;
3. substitution;
4. shuffling records;
5. number variance;
6. gibberish generation;
7. encryption/decryption.

Detailed technical discussion on those is out of scope for this chapter. Interested readers are urged to refer the white paper on *Data Sanitization Techniques* mentioned in the *Further Reading* section.

We summarize this section by noting that data sanitization or data masking is another technique for replacing sensitive data by realistic-looking false information. Data masking is the process of protecting sensitive information in non-production databases from inappropriate visibility. After sanitization, the database remains perfectly usable – the look-and-feel is preserved but the information content is secure. Data masking techniques work by applying some predefined simple and understandable rules to operate on the data. The collection of these rules forms what is known as a 'masking set'. Masking sets perform a series of known and repeatable actions.

5.11 Business Systems' Classification

We have discussed how organizations like to classify their information (Sections 5.6 and 5.7). Just like information and data of an enterprise or organization are classified, so are business systems in organizations. Table 5.2 presents the generally accepted classification. This concept is especially important in reference to the next chapter wherein we are going to discuss risk analysis for information systems security.

Table 5.2 | Business Systems' Classfications

Business systems' classification	Meaning
Critical	Functions supported by the system cannot be performed unless they are replaced by identical capabilities. Critical applications/systems cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, cost of interruption is very high.
Vital	Functions can be performed manually but only for a brief period of time. Higher tolerance to interruption than with critical systems and, therefore, lower cost of interruption provided restoration is within a certain time frame (usually a week).
Sensitive	Can be performed manually, at a tolerable cost, for an extended period of time. While it can be performed manually, it usually is a difficult process and requires additional staff to perform.
Non-critical	These functions may be interrupted for an extended period of time, at little or no cost to the company, and require little or no catching up when restored.

5.12 Event Classification

This will serve as an important reference for disaster recovery planning (DRP) and business continuity concepts in a later chapter of this book. This quick note here and Figure 5.4 are also an important reference to the next chapter. Events that can result in damage to IS are typically classified as:

1. **disaster**: an event that causes permanent and substantial damage or destruction to the property, equipment, information, staff or services of the business;
2. **crisis**: an abnormal situation that presents some extraordinary high risks to a business and that will develop into a 'disaster' unless carefully managed;
3. **catastrophe**: major disruptions resulting from the destruction of critical equipment in processing.

Figure 5.4 presents the relationship among various security-related terms.

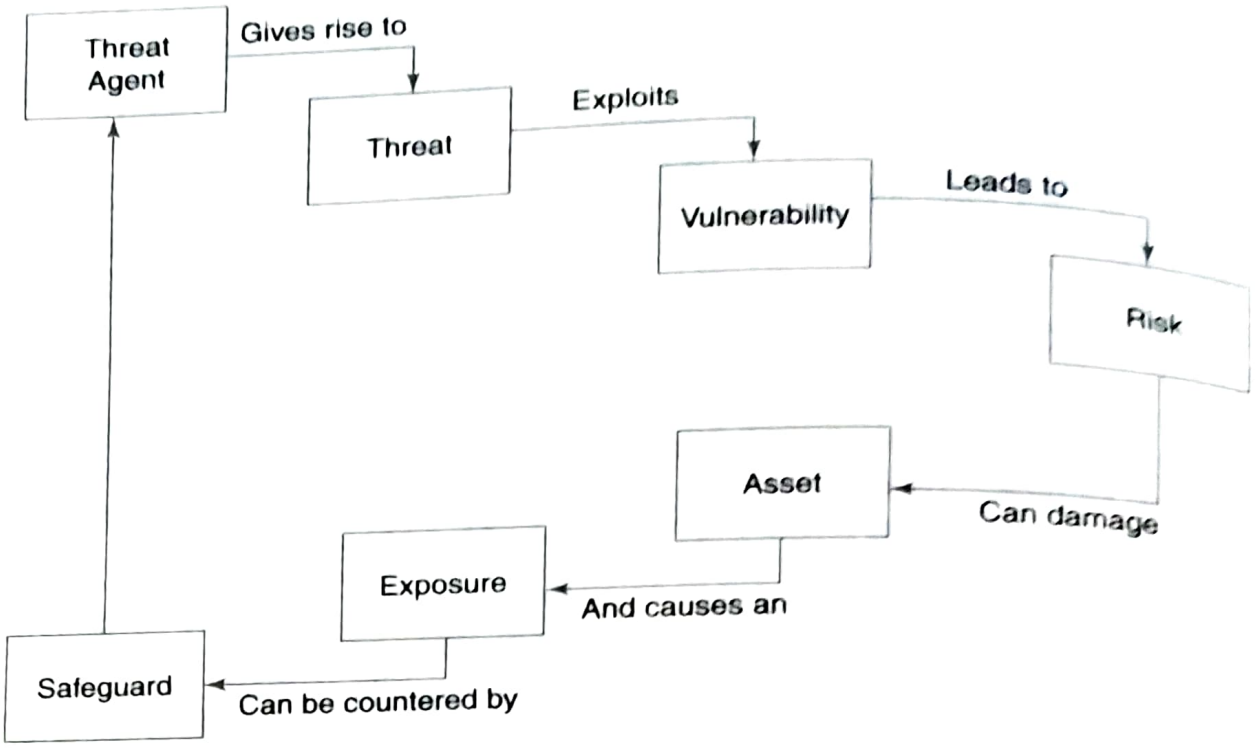


Figure 5.4 | Relationships among different security concepts.

Summary

The objective of this chapter was to provide a common reference on concepts for the next chapter. We started the discussion on various fundamental terms used in security-related topics. We discussed, important concepts in information classification as it forms a fundamental step toward information systems security. Classification of business systems and events was also addressed to serve as a foundation for a later discussion on disaster recovery (DR) and business continuity. We also mentioned about an interesting technique called data obfuscation that is a method not as strong as encryption but reasonably useful in some scenarios requiring protection of sensitive information. With this background, discussion on InfoSec risk analysis is taken up in the next chapter.

Review Questions

5.1 Explain the meaning of terms 'confidentiality', 'integrity' and 'availability'.

5.2 What is the difference between 'authentication' and 'authorization'?

5.3 Explain the considerations applied by organizations in classifying information.

5.4 What are the different roles involved in managing information as 'asset'? How does the role of 'custodian' differ from the role of 'user'?

5.5 Explain situations where data obfuscation turns out to be a useful technique than data encryption.

Mini Assignments

5.6 Study the infomation classification scheme in your work place or in the institute where you are studying.

5.7 Study the topic of 'data obfuscation' by visiting the white paper available at the URL quoted in the *Further Reading* section. Take a Microsoft Word document that you can lay your hand on. Obfuscate the word document. Record your observations, that is, whether you succeeded in obfuscation or not and the possible reasons for failure.

6 Information Security Risk Analysis

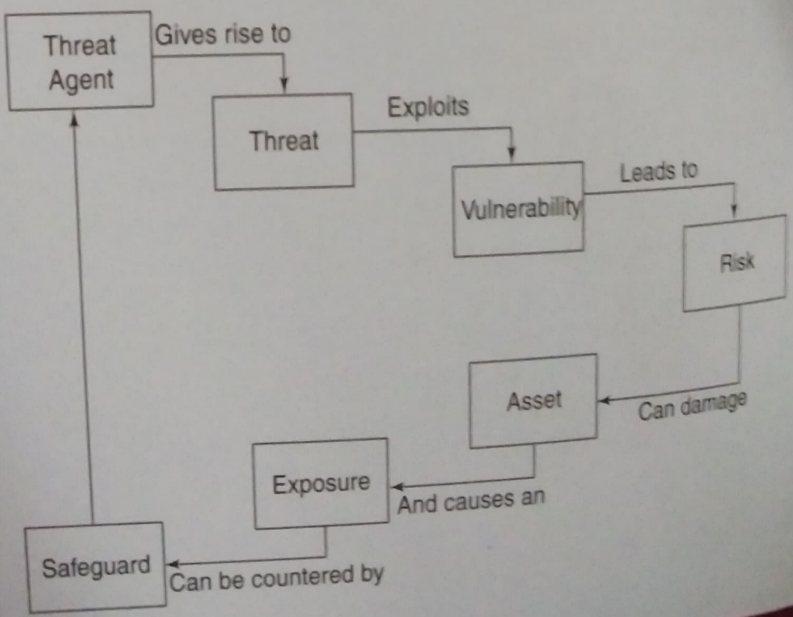
Learning Objectives

After completing this chapter you will be able to:

- develop an overall understanding about risk analysis for information security approach and considerations.
- capture key definitions involved in InfoSec risk analysis.
- understand the approaches to risk analysis, quantitative and qualitative.
- have a high-level overview of staged methodology for risk analysis.
- revisit asset classification.
- gain an understanding about InfoSec risk analysis from audit perspective.

6.1 Introduction

In Chapter 5, we covered the key concepts in building blocks of information systems (IS) [confidentiality, integrity, and availability (CIA); disclosure, alteration and destruction (DAD); etc.] also provided definitions of a few security-related terms: threats, vulnerabilities, risks, assets, exposure safeguards. Given that there are many sources of threats to information systems security, risk management becomes the cornerstone of information security (InfoSec) and that is the focus of this chapter. In this chapter, there will be a discussion about key points such as what risk management is, the need for risk management, approach to risk management, etc. Risk assessment will also be discussed in this chapter. In view of the role played by the IS in the global context and various threats to the IS (discussion in Chapters 1 and 2), this chapter is important. For the next section and in reference to Figure 6.1, an important point



remember is that combined with the security-related terms *asset* and *threat*, *vulnerability* is the third part of an element that is called a 'triple' in the domain of risk management, the main topic of this chapter.

6.2 Terms and Definitions for Risk Analysis of Information Security

Let us first discuss the concepts that appear in Figure 6.1. These terms and definitions form the basis for rest of the discussion in this chapter.

1. **Asset**: An asset is a resource, process, product, computing infrastructure and so on, something that an organization considers important so as to be protected. The loss of the asset could affect CIA (see Chapter 5) or could have an overall adverse business impact or it could have a discrete monetary value, either tangible or intangible. A compromised asset could affect the full ability of an organization to continue business, for example, a virus attack on its mail server system, damage caused to its software development facility owing to fire, earthquake or storm, etc. Remember the discussion in the previous chapter about classification of business systems (*critical*, *vital*, *sensitive* and *non-critical*) and classification of events (*disaster*, *crisis* and *catastrophe*). It is important to note that the value of an asset comprises all the elements that are related to that asset, its creation, development, support, replacement public credibility, associated costs and ownership values. For example, communication network, as an asset, consists of all the networking equipments: hardware and software, that is, routers, switches firewalls, etc. (details available in Chapters 12 and 15).
2. **Threat**: A threat is the presence of any potential event that could cause an adverse impact on the organization. It could be initiated by human beings (such as the malicious attacks on the websites) or natural (i.e., fire, earthquake, flood, etc.) and it can have a small or a large effect on the organization's security or viability.
3. **Safeguard**: A safeguard is the 'control' or 'countermeasure' put in place to reduce the risk associated with a specific threat or a group of threats. *InfoSec audits* are typically designed to check the presence of controls in place and their effectiveness, as will be discussed in Section 6.5.
4. **Vulnerability**: Vulnerability is the absence or weakness of a 'safeguard'. A minor threat has the potential to become a greater threat because of vulnerability. One way to understand this concept is to think of vulnerability as the threat that gets through safeguard into the system.
5. **Exposure-related terms**:
   - **Exposure factor (EF)**: The EF represents the percentage loss that a 'realized' threat event would have on a specific asset impacted by the threat. The EF value is needed to compute the *single loss expectancy* (*SLE*). SLE, in turn, is necessary to compute the *annualized loss expectancy* (*ALE*). The EF can be a small percentage, such as the effect of a loss of some hardware, or a very large percentage, such as the catastrophic loss of most storage devices at a data center (remember the event classification scheme discussed in the previous chapter).
   - **SLE**: An SLE is a monetary figure that is assigned to a single threat event. It represents an organization's loss from a single threat. It is derived from the following formula:

     $$\text{SLE} = \text{asset value (in monetary term)} \times \text{EF}$$

   - Let us understand this through a simple example: suppose you have an asset valued at USD 45,000 and say it is subjected to an EF of 20%. Then its SLE would be USD 900 (USD 45,000 × 0.2).
   - Note that while the monetary figure for the SLE is defined to arrive at the ALE value, it may at times be used for 'business impact analysis (BIA)' associated with 'disaster recovery planning (DRP)'. The topic of DRP is discussed in Chapter 34.

- **Annualized rate of occurrence (ARO):** This is the value that represents the 'estimated' possibility (probability) of a specific threat taking place within a one-year time frame. The range of probability is 0.0 (never) to 1.0 (always). The actual value can be anywhere within the range. For example, if the probability of storm-induced floods in the coastal Andhra (a state in India) region is once in 1,000 years, the ARO value is 0.001 (Box 6.1 has illustrations to explain the ARO concept.)
- **ALE:** The ALE value is a monetary value derived from the following formula:

$$ALE = SLE \times ARO$$

Box 6.1 Annualized Rate of Occurrence: Illustrations

Consider this: suppose a fire breaking out in a data center can cause a damage of Rs. 17,00,000 and the likelihood or ARO of a fire taking place has a value of 0.1 (indicating that the event is likely once in 10 years); then the ALE value is Rs. 1,70,000 = (Rs. 17,00,000 × 0.1).

Usefulness of the ALE concept is that it tells the organization the amount of money that is sensible to invest in designing 'controls' or 'safeguards' and employing them to prevent the feared damage from happening. In this example, it would not make a good business sense for the company to spend more than Rs. 1,70,000 to protect itself from the fire risk. Thus, it is important to know the real possibility of a risk and how much damage, in monetary terms, can be caused by the threat.

As another illustration, consider the following: suppose in a certain geographic center the probability of a volcanic eruption (in the vicinity) is estimated to be once every 100,000 years. Thus the ARO associated with this is 0.00001. In contrast to this, 100 data center operators attempting an unauthorized access could be estimated at six times a year per operator and therefore will have an ARO value of 600!

For a business enterprise, an asset can be of various types, for example, office premises, trade secrets, data storage equipments and servers, the data itself [more valuable than the server(s) on which they reside!] and customer-related information. Various risks can be associated with these assets: fire, theft, system failure, virus attacks, etc. Using the past data on the threats and taking clues from other organizations, companies can 'estimate' the possible damages if a threat event were to arise. This is the basic idea in InfoSec risk analysis.

The ALE is the annually expected financial loss to an organization from a threat. For example, a threat with a value of Rs. 10,00,000 (SLE) that is estimated to happen only once in 1,000 years (ARO value of 0.001) will result in an ALE of Rs. 1,000. This example shows us a more reliable way to cost/benefit analysis. Remember that the SLE is derived from the asset value and the EF. In Table 6.1, the concepts and formulae discussed are summarized.

Table 6.1 | Formulae for risk analysis

Exposure-related concept	Formula for calculation
Exposure factor (EF)	Percentage of asset loss caused by a threat
Single loss expectancy (SLE)	Asset value × EF
Annualized rate of occurrence (ARO)	Frequency of threat occurrence per year
Annualized loss expectancy (ALE)	SLE × ARO

6.3 Risk Management and Risk Analysis: What it is and the Need for it

In today's complex and over-extended work environment (remember the term 'extended enterprise' mentioned in Chapter 1 and Figure 1.2), one can see that risk management and risk analysis is not just another hot topic or buzzword or a fancy trend. Some people may think about it as just some activity to keep the administrative persons busy in an organization. However, the truth is far different. When used appropriately, that works as a foundation for a focused and solid countermeasure and planning strategy, risk management can provide key benefits and savings to a corporation. After the 9/11 tragedy (the tragedy that struck United States September 11, 2001 from a major terrorist attack), the world realized the importance of risk analysis and proactive risk tracking like never before. We now turn to the key discussion in this section.

Risk analysis is the science of observation, knowledge and evaluation – that is, keen eyesight, 'anticipation', etc. Risk management is the keystone to an effective performance as well as for targeted, proactive solutions to potential threats and incidents (an incident is any event that is not a part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service). Risk management is the ongoing process of identifying risks and implementing plans to address them. *Risk evaluation* is a process that generates an organization-wide view of InfoSec risks. It provides a baseline that can be used to focus mitigation and improvement activities. Many large organizations, to demonstrate their accent on risk management, are known to employ staff to hold the post of 'Chief Risk Officer'. Risk management is the skill of handling the identified risks in the best possible manner for the interests of the organization. Risk is described by the following mathematical formula:

$$\text{Risk} = \text{threat} \times \text{vulnerability} \times \text{asset value}$$

We did discuss some fundamental terms in the previous section in reference to Figure 6.1. Figure 6.2 illustrates the process for risk analysis/risk management. Relate the concepts shown in it to the discussion in Chapter 4 about the role of security policies and procedures.

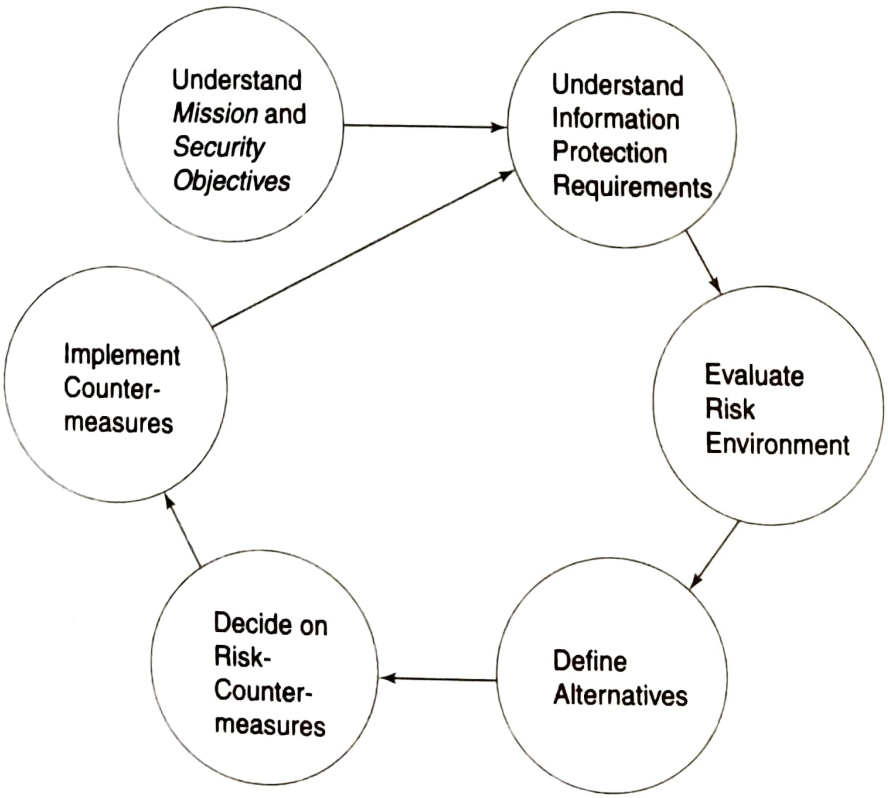


Figure 6.2 | Risk analysis/risk management process.

Staged Methodology for Risk Analysis

A 'methodology' is a framework for managing a task efficiently, usually including standard techniques for problem solving. For risk analysis, it will include taxonomy for data collection, a 'staged approach' (treating security planning like any other project), a method for analyzing data and some 'deliverables' or some appropriate 'measures of completion'. The three main stages in risk analysis are:

1. asset evaluation;
2. analysis of threats and vulnerabilities;
3. selection of safeguards.

Asset Classification

Basically, an 'asset' is anything that the organizations consider as a key component of their business process. Asset classification is necessary for asset evaluation. Assets are central to the theme of risk analysis. Therefore understanding asset classification is important. Chapter 5 had some discussion on this. Assets, being the central entity in risk analysis, let us understand how assets are categorized. Even though the information technology (IT) and businesses have evolved, asset categories have not changed much. This is not a problem because 'categories' are usually a starting point, not an objective for risk analysis methodology. As a result, asset definition is usually relatively inflexible and has an old-fashioned flavor. Information assets/IT assets usually fit into one of the following broad categories:

1. hardware;
2. software;
3. data;
4. documentation.

Sometimes, this list is extended to cover:

1. personnel;
2. procedures;
3. models;
4. communications equipment, that is, typically telecommunication (TC) network related;
5. logical data sets instead of physical files, network domains would also be considered here;
6. intangible aspects such as 'service' (remember the explanation of 'incident' provided earlier).

Figure 6.3 shows the main entities in a risk analysis model and their inter-relationships.

In reference to Figure 6.3, it is important to note that there are 'one-to-many' relationships involved: one vulnerability may result in many losses, one threat can create multiple impacts, etc. This figure mentions 'impact'; Box 6.2 has a note on *business impact analysis* (BIA) that is typically associated when DRPs are put into action. It also shows how BIA is related to risk analysis.

We summarize this section by making a note of some key points:

1. asset value;
2. impacts;
3. threats;
4. vulnerability;
5. asset loss exposures;
6. safeguards (countermeasures);
7. cost/benefit analysis.

Next, we cover the approaches to risk analysis.

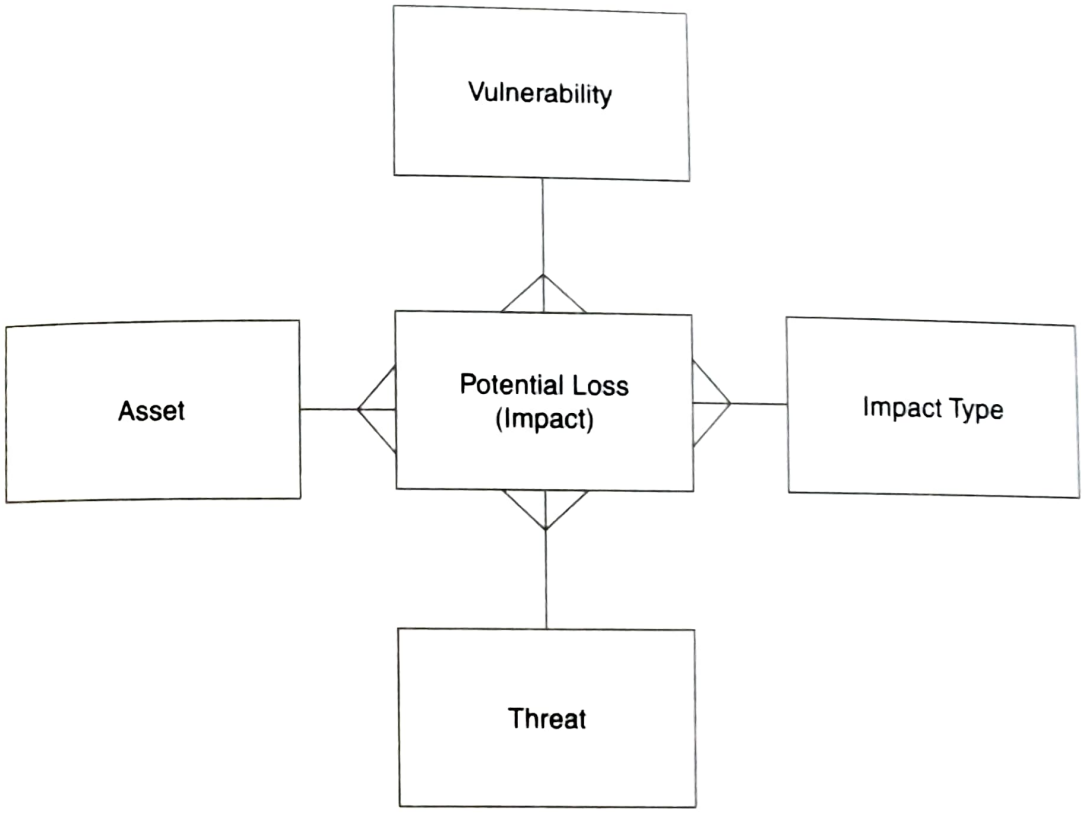


Figure 6.3 | Relationship among entities in risk analysis model.

Box 6.2 Business Impact Analysis

IS have multiple threats, each of which, when realized, can result in a disruption of IS/IT services. BIA is an assessment of the level of threat and the extent to which an organization is vulnerable to that threat.

One of the key steps in risk analysis is assigning a value to the assets that could be affected by each threat. This helps in establishing economic feasibility of the overall DRP. Once the DRP team knows about the possible threats and the amount of potential losses, it can arrive at the top key issues (say top 5–10 issues) and document this information for the management to clearly understand the threats faced by the organization.

These issues are a part of BIA that is a crucial first step in disaster recovery (DR) and contingency planning. Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted. Thus, the goal of the BIA is to see exactly how a business will be affected by different threats. The impact can be economic, operational or both. Typically, such information is gathered through standard survey tools or questionnaires administered on most knowledgeable/experienced people in the organization.

6.4 Approaches and Considerations in Information Security Risk Analysis

In this section, we are going to discuss the following:

1. quantitative risk analysis;
2. qualitative risk analysis;

3. valuation of IT/information system assets;
4. selection of safeguards.

How Quantitative Risk Analysis is Done

In *quantitative risk analysis*, the attempt is to assign independently the objective numeric values in monetary terms to the components of the risk assessment and to the assessment of potential losses. As against this, *qualitative risk analysis* addresses 'intangible values' of a data/information loss and its focus is on other issues rather than on the pure hard costs.

Risk analysis process is considered fully quantitative when all the elements of the risk analysis (asset value, impact, threat frequency, effectiveness, costs of safeguards/countermeasures, etc.) are measured, rated and values are assigned to them. In terms of practicalities of a business organization, 100% quantitative risk analysis is not possible. Qualitative measures, too, need to be applied. Thus, it should be noted that just because the figures look hard on reports it does not mean that it is possible to foretell the future with any certainty; uncertainty is a fact of life! (Box 6.3).

Box 6.3 Historical Perspective on Business Risk Analysis

Businesses have been analyzing risks as a routine part of their financing activity. This is typically done in terms of the relative risks involved in choosing among different patterns of investment, or whether or not to adopt some course of action such as developing a new project. This activity can be compared with evaluating IT/IS security risks. However, IT/IS security risk analysis is not as easy as business risk analysis. One reason for this being that it can have many limitations. The other reason is that often, adequate past data may not be available. The third and most significant factor is the technology obsolescence rate.

With IT/IS security, the challenge is that of evaluating potential loss against the cost of investing in a standard of security sufficient to reduce the risk to an acceptable level. This is because IT has come to be recognized as an asset in its own right recently. The problem is often magnified by uncertainty about benefits, that is, most of the times, the expected benefits can only be expressed in 'intangible terms', for example, 'company image', 'perception of stakeholders', 'assurance to customer', 'positive impact on customer goodwill', etc. Attaching a monetary value to such intangible benefits is not easy.

In the past, financial accountants understood computers as facilities that 'consumed funds'. However, since the value of computing performance was virtually unknown in earlier days, the accountants used to have a tendency to write off facility costs among the user departments.

The lack of historical data on IT assets has two important consequences: one is reflected in the large amount of time taken by the risk analysis exercise in an organization and the second effect is to ensure that the equivalent of the actuarial tables used in the normal insurance risk analysis cannot be developed.

A quantitative risk analysis process is like any other major project in the organizations and as such it requires a project or program manger to manage the main elements of the analysis. In reference to Figures 6.2 and 6.3, it is pertinent to note the risk analysis steps in the light of quantitative risk analysis:

1. Estimate the potential losses to the assets by determining their monetary value;
2. analyze potential threats to the assets;
3. define the ALE – see Table 6.1.

How Qualitative Risk Analysis is Done

A *qualitative risk analysis* does not attempt to assign costs to the elements of the loss. It is more of a 'scenario-oriented' approach and as such, in contrast to quantitative risk analysis, a 100% qualitative risk analysis is feasible. However, threat frequency and impact data are required to perform qualitative risk analysis.

In qualitative risk assessment, the seriousness of threats and the relative sensitivity of the assets are ranked, or a qualitative grading is provided to them, by using a scenario approach and creating an exposure rating scale for each scenario. During a scenario description, various threats are matched to the identified assets. A scenario is prepared to describe the type of threat and the potential loss to assets and the safeguards are selected to mitigate the risk. Table 6.2 shows the typical rating scales for exposures.

Table 6.2 | Scale for exposure rating

Rating level	Exposure percentage
0	No measurable loss
1	20% loss
2	40% loss
3	60% loss
4	80% loss
5	100% loss

Scenario Generation for Qualitative Risk Analysis

A qualitative risk assessment scenario begins after preparing 'threat listing' (based on asset classification and their role in business operations), list of assets to be covered under protection and assignment of exposure-level rating. The procedure for performing the scenario consists of the following steps:

1. documenting the scenario for addressing each major threat listed;
2. sanity check on the scenario through a review by the senior managers of the business units;
3. recommendation and evaluation of safeguards/countermeasures by the risk analysis team;
4. playing the scenarios and publishing the results to the senior management team responsible for the final decision.

After all the scenarios have been played out and the findings are published and submitted, the management is ready to implement the recommended safeguards/countermeasures as being acceptable and begins to seek alternatives for the safeguards that did not work (Box 6.4). Thus, one can see why risk analysis exercise needs to be treated like any other project. An example of a hypothetical qualitative risk analysis is presented in Table 6.3.

Box 6.4 **Model-Based Risk Assessments versus Asset-Based Risk Assessments**

Scope of protection includes systems and networks in addition to physical property and employee practices. Companies are moving beyond simple tools and quick patches to protecting information and improving corporate resilience strategies. Protecting a company includes not only its systems and networks but also its physical property and employee practices. Companies are moving beyond just buying vulnerability-checking tools and applying patches to protecting information. They are now

Box 6.4 *Continued...*

seeking ways to proactively improve corporate resilience rather than waiting to react to

vulnerability alert, thus there is a shift from a reactive approach to a proactive approach

This new posture is motivated in part not only by self-preservation but also by increasing

and regulatory pressures. InfoSec assessments have rapidly become a requirement in both

and industry-related domains. In the United States, the Gramm–Leach–Bliley Act (GLBA)

uniform resource locators (URLs) quoted in the *Further Reading* section] and the Health

Portability and Accountability Act (HIPAA) are driving efforts to improve corporate

to meet a defined standard of due care.

Reducing security risk is no longer a luxury; it is an essential part of business success.

assessments – such as Central Communication and Telecommunication Agency's Risk

Management Method (CRAMM), Consultative, Objective and Bi-Functional Risk

or any HIPAA-specific method (HIPAA is Health Insurance Portability & Accountability

– indicate how well your company can approach a designated ideal, but may not

Security certifications rely on predefined standards of what a secure system should be and

system developer's ability to define and implement the right operational security

Asset-based assessments, on the other hand, examine the information that must be

and how well systems and security practices provide that protection, thus providing a

of an organization's security posture. They look at the information that is critical to

objectives, and then examine the systems that support this information. Asset-based

answer the following questions:

1. What needs to be protected?
2. From whom and from what must it be protected?
3. How is it threatened?
4. What happens if it is not protected?
5. How can protection be improved?

A better approach is to combine assessment methods and techniques. A standard of due

such as HIPAA or International Organization for Standardization (ISO) 27000 (previously

can be embedded within asset-based assessments [such as Operationally Critical Threat,

Vulnerability Evaluation (OCTAVE®) described in Box 6.5] to measure compliance and

security improvement efforts.

Table 6.3 | Qualitative risk analysis example

Potential hacker	Threat severity	Threat probability	Potential loss	Effectiveness of firewall	Effectiveness of intrusion detection system	Effectiveness of Honey Pot
IT manager	4	2	4	4	3	2
Operational manager	5	4	4	4	4	2
Database administrator	4	4	4	3	4	1
Systems operator	3	4	3	4	2	1

Table 6.3 | Continued...

Potential hacker	Threat severity	Threat probability	Potential loss	Effectiveness of firewall	Effectiveness of intrusion detection system	Effectiveness of Honey Pot
Application programmer	2	3	3	4	2	1
Results	3.6	3.4	3.6	3.8	3.0	1.4

Note:

1. **Column 4 from left**: Scale of 1–5, where 5 represents the highest level of loss.
2. **Last row**: Average of the values in the column.
3. **Intrusion detection system (IDS)**: A software employed to monitor and detect possible attacks and harmful behaviors that vary from the normal expected activity (IDS is adderesed in Chapter 14).
4. **Honey Pot**: A system set up as a sacrificial lamb on the network in the hope that the attackers will attack this system instead of the actual system classified as critical to the business.

Box 6.5 Risk Analysis with OCTAVE Method

The OCTAVE® method (Operationally Critical Threat, Asset and Vulnerability Evaluation) is quickly becoming the de facto industry standard for InfoSec risk evaluations. It is a **risk-based strategic assessment** and planning technique developed by the Computer Emergency Response Team (CERT®) Coordination Center, a center of Internet security expertise operated by Carnegie Mellon University.

In its approach, OCTAVE method focuses on:

1. identifying critical assets of the organization and the threats to those assets;
2. identifying the vulnerabilities, both organizational and technological, that expose those threats, identifying risk to the organization;
3. developing a practice-based protection strategy and risk mitigation plans to support the organization's mission and priorities.

Creators of OCTAVE claim that most of the current risk assessment methods are 'bottom-up': they start with computing infrastructure and focus on the technological vulnerabilities without considering the risks to the organization's mission and business objectives.

According to CERT at Carnegie Mellon University, a better alternative is to look at the organization itself and identify what needs to be protected, determine why it is at risk and develop security measures requiring both technology- and practice-based solutions.

A comprehensive InfoSec risk evaluation approach:

1. incorporates assets, threats and vulnerabilities;
2. enables decision makers to develop relative priorities based on what is important to the organization;
3. incorporates organizational issues related to how people use the computing infrastructure to meet the business objectives of the organization;
4. incorporates technological issues related to the configuration of the computing infrastructure.

CERT recommends that risk analysis approach should use a flexible method that can be uniquely tailored to each organization.

Readers interested in exploring more details on the OCTAVE method are guided to the *Further Reading* section.

The main differences in the risk analysis approaches discussed (quantitative and qualitative) are laid out in Table 6.4.

Table 6.4 | Quantitative versus qualitative risk analyses

Parameter	Quantitative risk analysis	Qualitative risk analysis
Volume of information required	High	Moderate
Efforts involved	High	Moderate
Cost/benefit analysis	Yes	No
Accuracy of estimation/guess work	High/low	Low/high
Complexity of calculations	High	Moderate
Consideration to financial hard costs	Yes	No
Opportunity for using automated tools	High	Low
Ease of understanding	High	Low

Valuation of Assets

A simple tenet is that if information did not hold any value, then would organizations be interested to protect information assets? The value placed on information is almost always a matter of perception and is a relative concept involving: the number of entities involved, the efforts that have gone into the development of the asset and the total costs involved.

Both the types of risk analyses (quantitative and qualitative) as well as business impact risk analysis require the values of assets to be determined. A common mistake that the organizations can make is not to accurately identify the value of information before they implement security controls. The result is that often, the controls devised may not be suitable for asset protection (as subsequently revealed by security audits). Asset valuation is required for a number of reasons:

1. as a basis for cost/benefit analysis;
2. insurance-related and other statutory requirements;
3. for making decisions on selection of safeguards;
4. as a part of mandated 'due care' and to abide with legal requirements.

A number of factors are considered while performing asset evaluation:

1. usefulness and life-span of the asset;
2. initial one-time cost of the asset;
3. ongoing operational cost of the asset;
4. maintenance support cost of the asset;
5. hidden costs associated with the asset;
6. value of the intellectual property.

Selection of Safeguards

After completion of risk analysis, the next step is to perform a research on safeguards/countermeasures for protecting the critical information asset. Many standard principles are used to ensure that the selected safeguards match the threats envisaged (through either of the approaches to risk analysis – qualitative or quantitative); the important ones are mentioned as follows (full discussion on each of them is beyond the scope of this chapter):

1. cost/benefit analysis;
2. level of manual operations involved;
3. auditability/accountability features of the safeguard;
4. ability for recovery:
   - No destruction of asset while activation/reset of the safeguard;
   - no *covert channel* access to or through the control during reset (refer Chapter 11, Box 11.3);
   - ability to take default state so that the operators do not get any opportunity to manipulate or assume extra administrative rights until controls are fully operational.

We just make a note here that the covert channels are the means by which information can be communicated between two parties in a covert fashion using normal system operations. For example, by changing the amount of hard drive space that is available on a file server, the server can be used to communicate the information. Thus, covert channels are the communication channels that are not designed for any kind of information transfer, and yet they are still relevant in any shared environment. Another point to be noted is that covert channels are deeply linked to the security policy. For more information on this topic, readers are urged to use the *Further Reading* section.

6.5 Auditing Perspective on Information Security Risk Analysis

In this section, we discuss these two related, yet different professional practices. While 'auditing' and 'risk analysis' are congruent, they are *not* identical. In this section, our objective is to provide a brief overview of how the two practices are complementary and yet different in their approach. Although the two (IS auditing and InfoSec risk analysis) have common historical roots and considerable technical overlap at times, they differ in timing, perspective, subject matter and ultimate responsibility.

In general, the traditional electronic data processing (EDP) auditing can be defined as the activity of establishing reliability of information, that is, to establish that the transactions undertaken in reality correspond closely with the records that exist in the information system. Thus, a security auditor can form an adverse opinion if s/he is able to demonstrate that there are lapses in the controls in IS. When considering large and complex computer-based IS deployed in a network environment, the security auditors must proceed by evaluating the 'riskiness' of the system and its environment. This, in effect, is evaluation of (1) the strength of the system's built-in controls and (2) the extent to which people in the system's environment comply with procedural controls.

Good corporate governance depends on the effective management of internal controls and on the C.I.A. triad (confidentiality, integrity, and availability) of information within the organization. Corporate reputation, brand preservation and financial results all depend on the defense of business processes and on compliance with a growing array of legislation and regulation. For companies listed on US exchanges, the Sarbanes–Oxley Act (SOX) of 2002 is of overriding importance. In the digital 'net-centric' world of today, the corporate has its assets residing on the computer networks. The network has a fundamentally important role to play in SOX compliance, because it touches every aspect of the extended organization and connects business processes. The old, perimeter-based network security model is inadequate for managing security risks related to financial control information. The listed companies need an end-to-end system-based approach that is integrated, collaborative and adaptive, one that helps them better manage their network security risk while helping them meet SOX requirements (see Chapter 27 for details). In a compliant environment that, in addition to SOX, contains other overlapping, inconsistent, sometimes untested and often contradictory laws and regulations, organizations must increasingly turn to best practice solutions that combat their real-world information threats while helping them meet SOX and other regulatory requirements. International

Organization for Standardization (ISO) 17799 is one such framework. Well-guarded computers and networks provides the first line of corporate defense, because it is the foundation for the organization's data, applications and business processes—the protection of which is a prerequisite for SOX compliance.

Auditors analyze risks to determine how closely the system's controls comply with the standards recommended controls. Figure 6.4 shows how the security audit process begins by using risk analysis to determine whether the existing controls can be relied on even to the extent that they are worth reviewing at all. Given that by its very nature, auditing is an after-the-event activity and not a planning activity, auditors can test whether the defined controls are followed (compliance checking) but not the extent to which these controls should be applied in particular circumstances (adequacy checking).

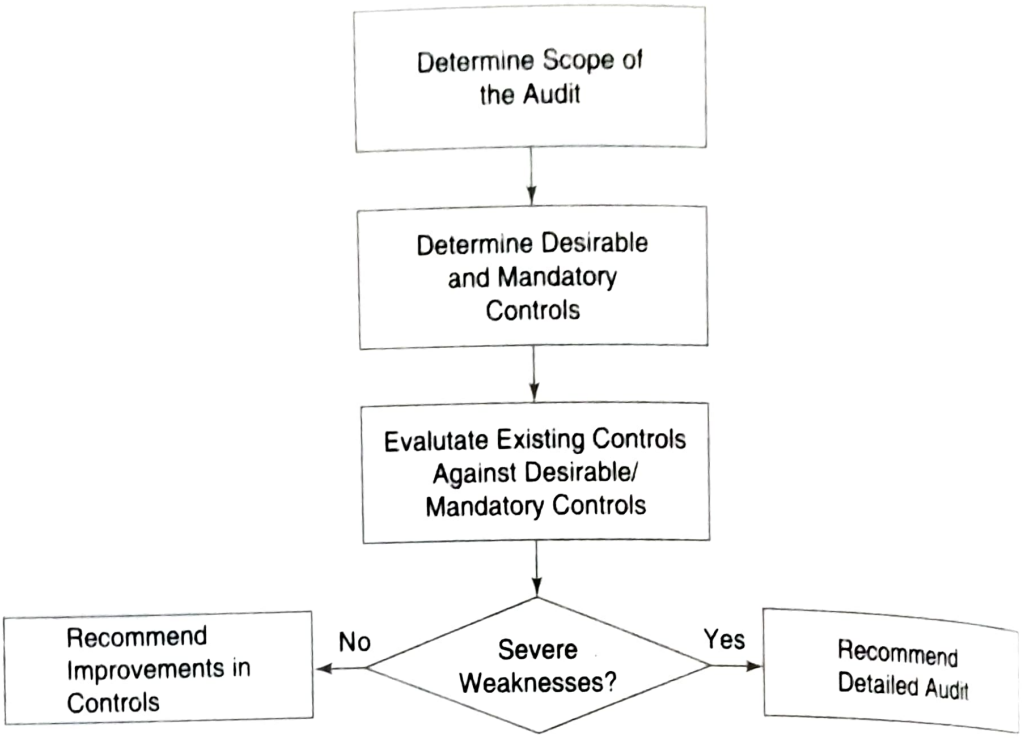


Figure 6.4 | Auditing perspective on risk analysis.

Auditors perform risk analysis in a legalistic context, and consider risk mainly to determine how much detailed auditing they must subsequently perform (i.e., to determine the need for substantive testing). Nevertheless, the methods and terminology developed by the auditors evaluate risk appearance, in some form, in most modern risk analysis methodologies (see Box 6.5). Annualized asset loss exposure, a concept discussed in Sections 6.2 and 6.3, has been an integral part of asset evaluation for many years. Between risk auditing and risk analysis, there are differences in subject matter too. The risk analyst tends to be more concerned with the infrastructure within which information assets are processed than with the assets per se, whereas security auditor's main preoccupation is with the control weakness that may be exposed through the IS audit.

Finally, we provide an end remark before concluding this section comparing the two professional practices (risk analysis vis-à-vis security auditing). In terms of relative responsibilities, the ultimate responsibility of the auditors of IS lies in the production of legally accurate financial statement (SOX of 2002 also emphasizes on this), if the audit is external, and the assessment of functioning of management controls, if the audit is internal. On the other hand, a risk analyst has a wider objective of successful accomplishment of the organization's security mission, working of its security policy, in regard to dynamic changes in business system environment. We thus conclude that both the disciplines are complementary and yet they differ in their approach.

3.5 Security Challenges Posed by Mobile Devices

Mobility brings two main challenges to the information systems security: on the handheld devices information is being taken outside of the physically controlled environment, and remote access back to the protected environment is being granted. Perceptions of the organizations to these security challenges are important in devising appropriate security operating procedure. When people are asked about important issues in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in Figure 3.6.

As the number of mobile device users increases, two challenges are presented; one at the device level – called 'Micro Challenges' and another one at the organizational level – called 'Macro Challenges'. Of these, some micro challenges are discussed in this section while the macro challenges are discussed in the next section.

Some well-known technical challenges in mobile security are: *managing the registry settings and configurations, authentication service security, cryptography security, lightweight directory access protocol (LDAP) security, remote access server (RAS) security, media player control security, networking application program interface (API) security, etc.* In Sections 3.6 and 3.7, we provide a brief discussion on these security aspects. For most of the discussion here, reference point is Windows mobile development given that the developers of the Windows OS are on the forefront of the technology in terms of their mobile computing technological initiatives. In view of the discussion in Section 3.4, the ID theft is now becoming a major fraud in credit card

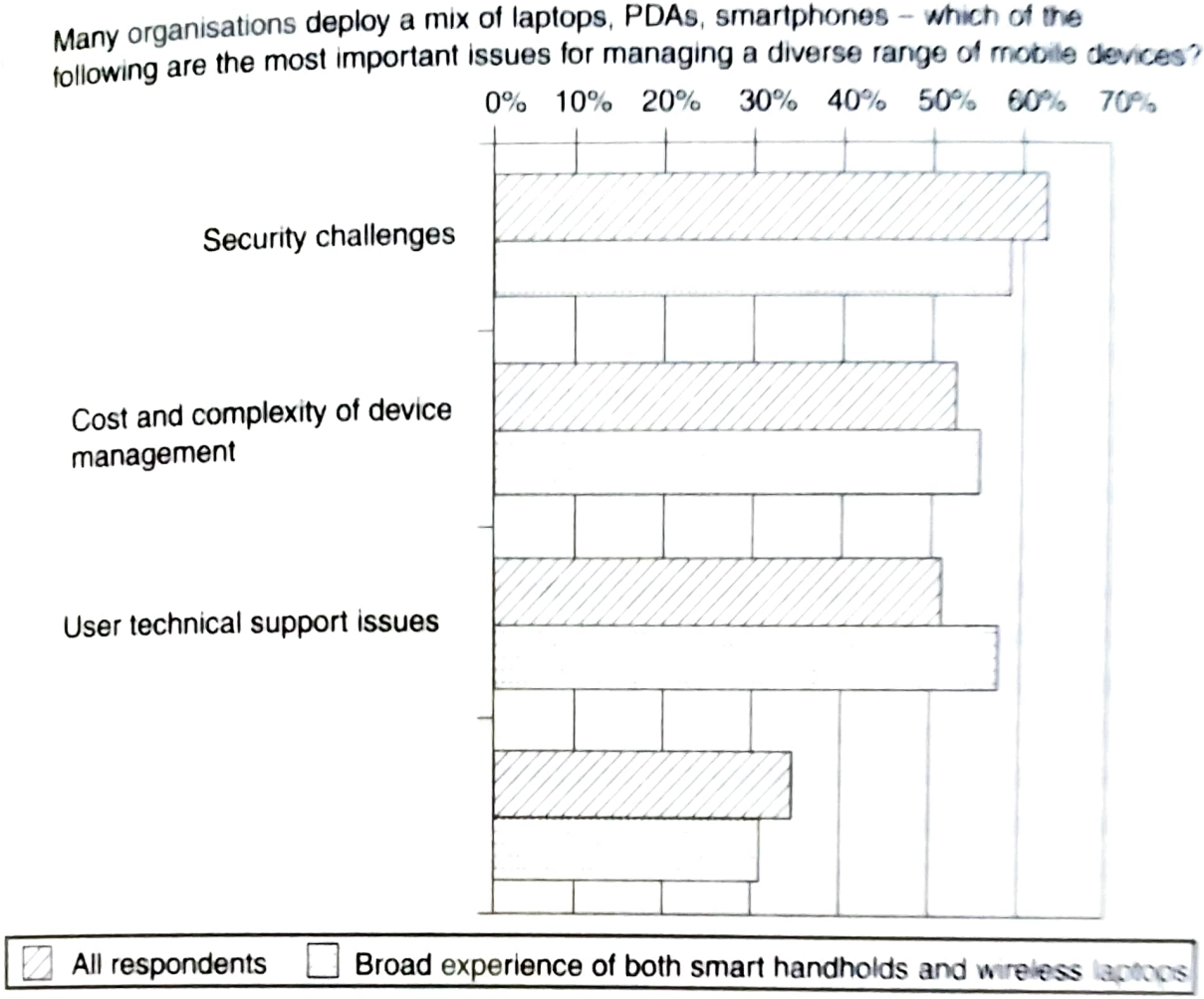


Figure 3.6 Important issues for managing mobile devices.
Courtesy: Mobile Devices and Users – Quocirca Insight Report, June 2005.

business domain; according to the Federal Trade Commission's (FTCs) report on 'Identity Theft' survey (year 2003), participants reported that in the last year they had discovered that their personal information (PI) had been misused to open new credit accounts, take new loans or engage in other types of frauds, such as misuse of the victim's name and identifying information when someone is charged with a crime, when renting an apartment or when obtaining medical care. A full discussion on this is beyond the scope of this chapter.