Chapter 15

Managing information security

CHAPTER AT A GLANCE

Main topics
- The need for controls 613
- Control strategies 619
- Types of controls 621
- Some techniques for controlling information systems 622
- Threats related to Internet services 632

Focus on ...
- The computer virus 626

Case studies
15.1 Passwords 624
15.2 Hackers 637

LEARNING OBJECTIVES

The learning objectives for this chapter are that readers should:
- be able to understand and assess potential threats to a computer-based information system;
- propose an overall strategy for ensuring the security of a computer-based information system;
- identify specific techniques that might be used to protect a computer-based information system against damage or unauthorised access.

MANAGEMENT ISSUES

The concept that information is an important and valuable business asset has been stressed throughout this text. The responsibility for ensuring the security of organisational information systems is one that cannot be taken too lightly. In addition to ensuring that the organisation has uninterrupted access to its information resources, managers must also deal with the threat of outsiders attempting to gain access to those same resources. From a managerial perspective, this chapter addresses the following areas:
- An understanding of approaches towards information systems security will help managers to develop and implement an overall strategy for security.
- An understanding of the threats to information systems will help in predicting and anticipating acts such as denial of service attacks.
- Knowledge of specific techniques for protecting information systems will help in the development of effective countermeasures.
- As organisations turn to the Internet for business purposes, it becomes important to understand some of the new threats that must be faced.
Activities

Activity 15.1 (P. 624)
Using the Internet as a resource, locate information related to a well-known product called Pretty Good Privacy (PGP). Describe how PGP works and explain why you think the system is so popular.

PGP uses a private-key, public-key system to ensure security. The public key is available to anyone and can be attached to e-mail messages, data files and so on. However, unless the recipient has access to the sender’s private key, the data cannot be decrypted. PGP users can have as many public and private keys as they desire, allowing them to use different keys for different purposes. As an example, an individual might use one set of keys for personal messages and another for business communications. Although somewhat cumbersome, this approach works well once the appropriate keys have been created and registered.

There are three main reasons why PGP is popular:
- The software is available free of charge (note that commercial versions of PGP are also available).
- The encryption method (algorithm) used is considered very robust, providing users with a high level of security.
- Once configured, the software is relatively easy to use and, in some cases, works transparently (that is, users are almost unaware of the software’s operation).

Activity 15.2 (P. 632)
Using the Internet as a resource, locate three examples of recent denial of service attacks. For each example, describe how the attack occurred and the losses suffered by the victim.

There is no solution for this activity since it is a research-based task.
Case Studies

**Case Study 15.1: Passwords (P. 624)**

1. Why should an organisation use passwords to protect equipment and sensitive data from unauthorised users?

2. The case study describes several ways in which fraudulent users are able to obtain important passwords. What measures can an organisation take to protect against some of the methods described?

3. Describe the password protection features provided by a typical operating system, such as Windows NT.

1. It is important to recognise a number of points:

   • Most of the hardware and software used by a company will support the use of passwords. This means that password protection is simple and inexpensive to implement.

   • It is important to remember that password methods are not intended solely for the protection of data. It is more accurate to suggest that password protection is used to prevent unauthorised access to a company’s hardware, software and data resources.

   • For many industries, it is important to gain the public’s confidence. For this reason, password protection is often used to satisfy the public that sensitive data is held to be confidential.

   • Password protection is also used as a simple means of meeting some of a company’s legal and contractual obligations. As an example, companies must meet stringent security requirements before they can be awarded certain government contracts. Companies also have a legal and moral duty to ensure that sensitive data is viewed only by authorised personnel.

2. Using the case study, students should be able to identify a number of measures that can be taken to prevent unauthorised persons from obtaining passwords. Some examples include:

   • The ‘social engineers’ described in the case study can be defeated using a number of very simple methods. A common approach involves using ‘code words’ agreed between the company and its clients. Passwords are only divulged when the correct code word is given during the telephone call. A second approach involves recording the details of a request for a password and then telephoning the company or individual to confirm their identity.

   • The only effective way of defeating ‘dumpster divers’ is to set a company policy that prohibits users from writing their passwords down. However, in order for such a policy to be effective it must be widely publicised and strictly enforced.

   • In many organisations, such as banks, screens are used to prevent ‘shoulder surfers’ from viewing information displayed on a monitor.

   • Although password-cracking programs can be extremely effective in finding passwords through a ‘brute force’ approach, the task can be made more difficult by using relatively long passwords and by choosing passwords that cannot be guessed easily. As an example, many people use birthdays, middle names, maiden names and even car registrations as their passwords. Such passwords are easily guessed, even without using a password-cracking program. Once again, the only effective way of minimising the risk posed by password-cracking programs is by educating users and providing guidance in the form of a company security policy.
3. An operating system such as Windows XP or Windows 2000, provides several password protection features. Amongst these are:
   - The Windows startup sequence can be made to ask a user for a password before they begin working with the machine. A number of actions can be taken, depending on the password entered. For example, a default password can be used to allow some users to word process or use a database package. However, only a specific user password may allow access to a given disk drive or program.
   - Windows can also restrict access to network resources according to the password entered. This can be used to protect data held on a network server, or even to restrict access to resources such as printers and modems.
   - Screen savers can be used to blank the computer’s monitor whilst the user is away. This hides any sensitive information currently on the screen and the machine can only be used when the correct password is entered.

Case Study 15.2: Hackers (P. 631)

1. Why are firewalls ‘like putting a steel door on a cardboard house’?
2. What methods can be used to defeat techniques such as the use of programs that generate passwords or calling the IT department to have a password reset?
3. Should we distinguish between ‘white hat’ and ‘black hat’ hackers, or are all hackers the same?

1. The case study points out that many threats to information systems arise from within the organisation. Firewalls cannot protect against a disgruntled employee carrying out an act of sabotage, or making copies of valuable data. In addition, many companies rely on firewall software alone to protect against network intrusions. In the event that the company's network is infiltrated, other methods must be used to detect intruders.

2. Several methods can be used to defeat these techniques. Some examples include:
   - User validation routines can prevent entry to the information system even if the correct password is known.
   - Procedures to be carried out when a password is lost or forgotten can be improved to prevent passwords being reset under false pretences. For example, support staff might be required to call a user back in order to verify a request to reset a password.
   - Intrusion detection software can be used to detect attempts to guess passwords by brute force. For example, if more than three attempts are made to enter a password, an alert can be automatically sent to support staff.
   - Attempts at entering passwords can be limited by using the facilities that already exist within modern hardware and software. For example, many personal computers "lock up" if a password is entered incorrectly more than three times.

3. Some of the points that might be discussed include the following:
   - Hacking involves gaining unauthorised access to an information system. Irrespective of the motivation behind such acts, they are illegal and might cause damage to the information system.
• Some people believe in the idea of "poacher turned gamekeeper", assuming that it often takes one skilled hacker to catch another skilled hacker. If this view is taken, we must accept the existence of both "good" and "bad" hackers.

• There can be no doubt that some hackers serve the public interest (whether intentionally or otherwise). For example, there have been many cases where hackers have helped to pursue child pornographers, drug runners and other criminals. It is unfair to regard these people in the same light as a hacker who, for example, defaces a web site.

• As described by the case study, companies can make use of hackers in order to test and improve their network defences. Again, if this view is taken, we must accept the existence of both "good" and "bad" hackers.
Exercises (PP. 637 – 639)

Self-assessment exercises

1. What are the two basic reasons for the need to control computer-based information systems?

The two basic needs for controls are the need to ensure the accuracy of the data held by the organisation and the need to protect against loss or damage.

2. List some of the advantages and disadvantages of using passwords to protect equipment and sensitive data from unauthorised users.

From the text, some of the advantages of using passwords include:
- Access to the system can be divided into levels by issuing different passwords to employees based on their positions and the work they carry out.
- The actions of an employee can be regulated and supervised by monitoring the use of their password.
- If a password is discovered or stolen by an external party, it should be possible to limit any damage arising as a result.
- The use of passwords can encourage employees to take some of the responsibility for the overall security of the system.
- Password protection is relatively simple and inexpensive to implement.

Some disadvantages include:
- In order to ensure the highest level of security, all users must take care to choose appropriate passwords and ensure that they are not disclosed to others.
- By themselves, passwords do not provide an extremely high level of security. As shown in the relevant case study, there are many ways in which password protection can be circumvented.
- Even when used on a comparatively small scale, passwords can dramatically increase the demands made on support staff. Lost or forgotten passwords, for example, represent one of the most common requests made to support staff.

3. What types of controls can be used to protect a computer-based information system against vandalism, theft and unauthorised access?

The basic categories of controls are:
- physical protection;
- biometric controls;
- telecommunications controls;
- failure controls;
- auditing.
4. What are the advantages and disadvantages of an approach to controlling computer-based information systems that is based on containment?

Some advantages include:
• Such an approach provides a great deal of flexibility since a number of different techniques can be used in combination to increase the level of protection.
• This approach is particularly suited to certain kinds of organisation. Large national or multinational organisations, for example, often have their IT resources dispersed across a large geographical area, making it easier to isolate specific resources or distribute important assets more widely.

Some techniques, such as encryption, are simple and inexpensive to implement.

Some disadvantages include:
• The defences erected must be continually monitored and improved.
• In some cases, isolating important systems or distributing data more widely can have an impact on the organisation’s effectiveness.
• In general, a policy of containment is expensive to implement and maintain.

5. Describe some of the ways in which accidental damage can occur to a computer-based information system.

Some of the most common causes of accidental damage include:
• inaccurate data entry.
• attempts to carry out tasks beyond the ability of the employee.
• failure to comply with procedures for the use of organisational information systems.
• failure to carry out backup procedures or verify data backups.

6. Explain why virus scanning software and anti-virus programs are often of only limited value in detecting and removing computer viruses.

Some of the reasons for this are:
• Virus detection programs must be continually updated otherwise they are unable to detect new types of computer virus.
• Some types of computer virus, such as ‘polymorphic’ viruses, can alter their structure so that they are not easily detected.
• Some types of computer viruses are engineered to evade detection by specific virus scanning programs.
• In tests, no virus detection program has yet achieved a perfect score, meaning that no virus detection program is completely effective.
Discussion questions

1. What motivates an individual or organisation to create a computer virus?

Some of the motives that students might wish to explore include:
- Revenge, for example against a former employer.
- Financial gain, for example through criminal acts such as extortion.
- Competitive reasons, for example it is suggested that some people create viruses in order to ‘defeat’ the programmers of virus detection programs.
- It has been alleged that computer viruses are created as a means of industrial sabotage or as an act of terrorism.

2. No computer-based information system can be considered completely secure – all organisations should base their control strategies on recovery. Make a case in favour of or against this argument.

Students may wish to consider some of the following points:
- A policy based on recovery means that the organisation is willing to accept damage to valuable equipment and data. In the long term, this may be more expensive than attempting to prevent such damage in the first place.
- Unless some form of action is taken to deter unauthorised access, companies will actually increase the severity of the problem.
- Ultimately, the security of a company’s hardware, software and data resources relies on the intelligence and skills of those charged with protecting them. There will always be at least one hacker that is more skilled and more intelligent than the company's employees. This means that it is impossible to create a series of defences that provide complete security.
- If a company’s defences will be breached anyway, there is no reason to waste time, money and other resources on creating ineffective barriers. Surely, it is more sensible to divert these resources towards recovering from a security breach? In this way, the company will be able to recover more quickly and more fully.

3. ‘An increased reliance on the Internet exposes organisations to increased risk in terms of threats to information systems security.’ Make a case in favour or against this argument.

Some of the issues that students should consider include:
- As soon as an information system becomes connected to the Internet, the level of threat is increased because the system is now prone to attack from outside the organisation.
- Increased reliance on the Internet as a means of conducting business transactions means that potential losses may be larger if the organisation is deprived of its Internet services.
- Increased reliance on the Internet increases the risk posed by threats such as Denial of Service attacks; such threats would cause little harm to an organisation that conducts most of its transactions offline.
• Does an increased reliance on the Internet as a business tool also mean increased reliance on Internet security tools, such as firewalls? Just how good is Internet security? Is it likely that a firewall or intrusion detection package will be able to deflect every possible attack?
Essay questions

1. Conduct any research necessary and produce a formal security policy governing student access to the computer systems at the institution that you attend. In addition to providing details of any controls already in place, your work must also address the areas listed below. For each of these areas, you should also justify any decisions or choices made.

(a) what activities are considered acceptable;
(b) what activities are considered unacceptable;
(c) the sanctions that may be used against those failing to comply with the policy.

(a) Typically, an institution will describe a number of specific activities that are considered acceptable and will state that any activity not mentioned should be considered unacceptable. Some of the activities described will include:

- Use of applications software for activities related to academic study: word processing, spreadsheets, use of CD-ROM materials, and so on.
- Use of the Internet for research purposes.
- Use of printing facilities for documents related to academic study.
- Use of e-mail software to contact academic staff and in support of academic research.

(b) In general, a number of specific items will be listed together with a more general statement of policy. The items listed may include:

- Students must not disclose their passwords or allow others to use their network accounts.
- Students must not use the institution's facilities in support of activities not related to the student's course of study.
- Students may not install or use leisure software (games).
- Students may not view or download pornography, illegal software or games. In addition, students will be warned against copying or downloading copyrighted materials.
- Students must not carry out any activity that causes harassment of any kind, including racial and sexual harassment.
- Other prohibited activities may include theft, physical damage and attempts to view or modify confidential data held by the institution.

Institutions may also produce a more general statement that prohibits any activity considered illegal under the Data Protection Act or Computer Misuse Act. Such a statement will normally be accompanied by a list of the activities specifically mentioned by each piece of legislation.

(c) Typically, the sanctions imposed against those in breach of the institution's policies will include:

- a formal warning that may lead to further sanctions in the future;
- temporary or permanent suspension of the student’s right to use the institution’s facilities;
- temporary or permanent expulsion from the institution;
- prosecution under criminal or civil law.
2. Select an organisation that you are familiar with, such as a university or bank. Conduct any research necessary to address the following tasks:
(a) Describe the potential impact of infection by computer viruses on the organisation’s computer-based information systems.
(b) Consider the effectiveness of tools, methods and procedures designed to protect computer-based information systems from computer viruses.
(c) Evaluate the level of risk posed to the organisation by computer viruses and produce a set of recommendations that may assist the organisation in reducing this risk.

(a) In general, all organisations will suffer losses arising from three basic areas:
- Damage to important data.
- Loss of access to important hardware, software and data resources.
- Inability to carry out normal activities.

(b) Students should consider a wide range of areas. Some of these areas may include:
- The effectiveness of any existing virus detection software used by the company.
- Whether or not company procedures work to reduce the risk of virus infections.
- How effective the company's recovery plans are likely to be.

Students should relate their material to a general discussion of the effectiveness of virus detection software.

(c) In general, the level of risk to all but the smallest companies remains high. A student's response should recognise this and should use the figures and information provided in the text to support their arguments. This material can also be used to develop a series of recommendations that will act to reduce the level of risk to the company.

In particular, students should deal with issues such as ensuring that employees:
- do not "carry" computer viruses from personal computers to the company's information systems.
- know how to recognise the signs of an infection by a computer virus.
- understand what action should be taken if a virus infection is discovered.

3. Outline some of the threats to information systems that arise as a result of doing business via the Internet. Illustrate your response with appropriate examples and indicate how the risks you identify can be mitigated.

Students should refer to the final part of the chapter for an overview of common threats faced by organisations that do business via the Internet. A good response will describe and discuss issues such as denial of service attacks, identity theft, brand abuse, fraud, cyberterrorism and cyberstalking.

In general, students should describe an approach to security that includes the following points:
- The use of appropriate software such as antivirus packages, firewalls and intrusion detection software.
- The implementation of a formal security policy that incorporates an acceptable use policy.
• The use of regular audits to control activities such as the use of illegal software. Audits can also be useful in detecting unauthorised access to data and attempts to carry out acts of fraud.
• The introduction of various recovery methods intended to allow the organisation to resume its operations as quickly as possible. In the context of an organisation that relies on the Internet as a business tool, this might include access to backup servers so that essential administrative processes (e.g. e-mail) and e-commerce facilities (e.g. customer ordering facilities) are restored quickly.
Examination questions

1. Computer viruses represent a significant threat to the security of organisational computer-based information systems. It is estimated that as many as 500 new computer viruses appear each month. You are required to:
   (a) Provide a definition of the term ‘computer virus’.
   (b) Using relevant examples, describe the ways in which computer viruses can be transmitted.
   (c) Discuss some of the ways in which organisations can protect against computer viruses. Highlight some of the advantages and disadvantages of each method described.

(a) The text provides the following definition for a computer virus:
   *A computer virus is a computer program that is capable of self-replication, allowing it to spread from one ‘infected’ machine to another.*

(b) The student’s response should deal with some or all of the following:
   • Via software downloaded from the Internet.
   • Via disks or other media used with an infected personal computer and then returned to the company’s information systems.
   • Deliberately released into the company’s information systems, perhaps by a disgruntled employee.
   • Via infected software distribution media.
   • Via illegal (‘pirate’) software used on the company’s information systems without proper authorisation.

(c) The student’s response should discuss some or all of the following approaches:
   • The installation of virus detection software.
   • The introduction of formal policies, for example, a formal security policy.
   • Education and training designed to alert employees to the threat posed by computer viruses and allowing them to recognise the signs of infection and react accordingly.
   • Regular audits of software and company-wide scanning of software and data files.
   • If not already implemented, a procedure for making regular backups of important data.

2. With regard to the control of computer-based information systems, answer the following:
   (a) Describe some of the common security threats facing organisational computer-based information systems.
   (b) Explain the four basic approaches to controlling computer-based information systems. Highlight the advantages and disadvantages of each approach.
   (c) More effective protection for a computer-based information system can be achieved by employing a combination of the four basic approaches to control. Using relevant examples, discuss this statement.

(a) The most common threats to information systems are:
• accidents;
• natural disasters;
• sabotage (industrial and individual);
• vandalism;
• theft;
• unauthorised use (hacking);
• computer viruses.

(b) The four basic approaches to controlling computer-based information systems are:
• 
  Containment: attempting to control access to an information system.
• Deterrence: using the threat of punishment to discourage potential intruders. The overall approach is one of anticipating and countering the motives of those most likely to threaten the security of the system.
• Obfuscation: hiding or distributing assets so that any damage caused can be limited.
• Recovery: recognising that, no matter how well defended, a breach in the security of an information system will eventually occur. This approach attempts to ensure that the normal operation of the information system is restored as quickly as possible, with minimal disruption to the organisation.

(c) Students should demonstrate an understanding of the weaknesses of each approach described in (b). Using relevant examples, the student should attempt to demonstrate how a combination of the four basic control strategies will provide the highest level of protection against damage and unauthorised access.

3. A formal security policy can provide an effective means of protecting an organisation’s computer-based information systems against theft, damage and other hazards.

(a) Provide an overview of the areas that will be outlined by a typical formal security policy document.

(b) Describe the ways in which a formal security policy can help to protect an organisation’s computer-based information systems.

(c) A number of factors will determine whether or not a security policy works effectively. Using relevant examples, provide a brief discussion of some of these factors.

(a) A formal security policy document will typically contain the following basic sections:
• what is considered to be the acceptable use of the information system;
• what is considered to be the unacceptable use of the information system;
• the sanctions available in the event that an employee does not comply with the security policy;
• details of the controls in place, including their form, function and plans for developing these further.

(b) Some of the areas that students might discuss include:
• Setting in place procedures, such as regular backups of data, that will help to improve security.
• Helping to ensure that users understand which actions are acceptable and which are not.
• Educating users so that they can recognise and respond to threats.
• Setting out guidelines that help and educate employees so that they are able to use information systems safely and responsibly.
• Publicising the sanctions that will be used against those responsible for a breach of security.

(c) Some of the factors that will influence whether or not a policy is successful include:
• Whether or not the policy is comprehensive and deals with the majority of the issues relevant to the company.
• Whether or not managers support and enforce the rules and procedures set out in the policy.
• Whether or not the sanctions available to managers are used consistently and responsibly.
• The way in which the policy is implemented, for example publicity will be required to ensure that all employees understand that a policy exists.
• Whether or not employees receive adequate training and guidance, so that they understand the importance of the policy and their responsibilities.