10 Information Systems Security

The role of computer controls and security is to protect systems against accidental mishaps and intentional theft and corruption of data and application, as well as to help organisations ensure that their IT operations comply with the law and with expectations of employees and customers for privacy (Oz and Jones, 2008). This section discusses security threats to information systems before introducing methods to protect information systems against these threats. A particular emphasis is placed on the areas of computer viruses and threats to Internet services.

10.1 Security Threats to Information Systems

Controls upon information systems are based upon the two underlying principles of the need to ensure the accuracy of the data held by the organisation and the need to protect against loss or damage. The most common threats faced by organisational information systems can be placed into the following categories of accidents, natural disasters, sabotage (industrial and individual), vandalism, theft, unauthorised use (hacking) and computer viruses which will now be described.

10.1.1 Accidents

A number of estimates suggest that 40–65% of all damage caused to information systems or corporate data arises as a result of human error. Some examples of the ways in which human errors can occur include:

- *Inaccurate data entry*. As an example, consider a typical relational database management system, where update queries are used to change records, tables and reports. If the contents of the query are incorrect, errors might be produced within all of the data manipulated by the query. Although extreme, significant problems might be caused by adding or removing even a single character to a query.

- *Attempts to carry out tasks beyond the ability of the employee*. In smaller computer-based information systems, a common cause of accidental damage involves users attempting to install new hardware items or software applications. In the case of software applications, existing data may be lost when the program is installed or the program may fail to operate as expected.

- *Failure to comply with procedures for the use of organisational information systems*. Where organisational procedures are unclear or fail to anticipate potential problems, users may often ignore established methods, act on their own initiative or perform tasks incorrectly.

- *Failure to carry out backup procedures or verify data backups*. In addition to carrying out regular backups of important business data, it is also necessary to verify that any backup copies made are accurate and free from errors.

10.1.2 Natural disasters

All information systems are susceptible to damage caused by natural phenomena, such as storms, lightning strikes, floods and earthquakes. In Japan and the United States, for example, great care is taken to protect critical information systems from the effects of earthquakes. Although such hazards are of less concern in much of Europe, properly designed systems will make allowances for unexpected natural disasters.

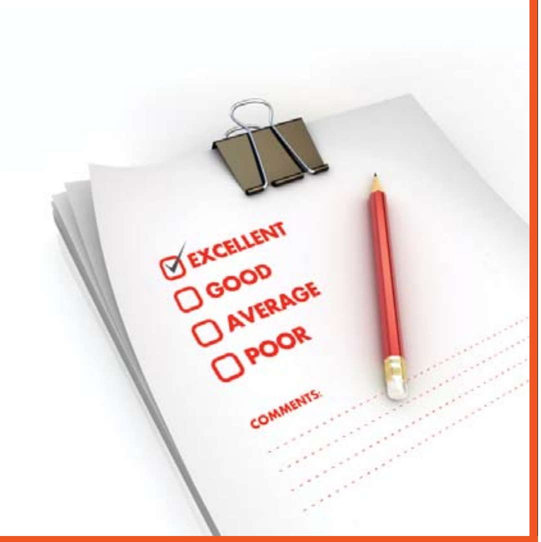
10.1.3 Sabotage

With regard to information systems, sabotage may be deliberate or unintentional and carried out on an individual basis or as an act of industrial sabotage. Individual sabotage is typically carried out by a disgruntled employee who wishes to exact some form of revenge upon their employer. The logic bomb (sometimes known as a 'time bomb') is a well-known example of how an employee may cause deliberate damage to the organisation's information systems. A logic bomb is a destructive program that activates at a certain time or in reaction to a specific event. In most cases, the logic bomb is activated some months after the employee has left the organisation. This tends to have the effect of drawing suspicion away from the employee. Another well-known example is known as a back door. The back door is a section of program code that allows a user to circumvent security procedures in order to gain full access to an information system. Although back doors have legitimate uses, such as for program testing, they can also be used as an instrument of sabotage. It should be noted, however, that individual sabotage is becoming more infrequent due to legislation such as the Computer Misuse Act.

Industrial sabotage is considered rare, although there have been a number of well-publicised cases over the past few years. Industrial sabotage tends to be carried out for some kind of competitive or financial gain. The actions of those involved tend to be highly organised, targeted at specific areas of a rival organisation's activities, and supported by access to a substantial resource base. Industrial sabotage is considered more serious than individual sabotage since, although occurrences are relatively few, the losses suffered tend to be extremely high. An intent to cause loss or damage need not be present for sabotage to occur. Imagine the case of an organisation introducing a new information system at short notice and without proper consultation with staff. Employees may feel threatened by the new system and may wish to avoid making use of it. A typical reaction might be to enter data incorrectly in an attempt to discredit the new system. Alternatively, the employee might continue to carry out tasks manually (or with the older system), claiming that this is a more efficient way of working. In such cases, the employee's primary motivation is to safeguard their position the damage or loss caused to the organisation's information systems is incidental to this goal.

10.1.4 Vandalism

Deliberate damage caused to hardware, software and data is considered a serious threat to information systems security. The threat from vandalism lies in the fact that the organisation is temporarily denied access to some of its resources. Even relatively minor damage to parts of a system can have a significant effect on the organisation as a whole. In a small network system, for example, damage to a server or shared storage device might effectively halt the work of all those connected to the network. In larger systems, a reduced flow of work through one part of the organisation can create bottlenecks, reducing the overall productivity of the entire organisation. Damage or loss of data can have more severe effects since the organisation cannot make use of the data until it has been replaced. The expense involved in replacing damaged or lost data can far exceed any losses arising from damage to hardware or software. As an example, the delays caused by the need to replace hardware or data might result in an organisation's being unable to compete for new business, harming the overall profitability of the company. In recent years, vandalism has been extended to the Internet. A number of incidents have occurred where company web sites have been defaced.



10.1.5 Theft

As with vandalism, the loss of important hardware, software or data can have significant effects on an organisation's effectiveness. Theft can be divided into two basic categories: physical theft and data theft. Physical theft, as the term implies, involves the theft of hardware and software. Data theft normally involves making copies of important files without causing any harm to the originals. However, if the original files are destroyed or damaged, then the value of the copied data is automatically increased. Service organisations are particularly vulnerable to data theft since their activities tend to rely heavily upon access to corporate databases. Imagine a competitor gaining access to a customer list belonging to a sales organisation. The immediate effect of such an event would be to place both organisations on an essentially even footing. However, in the long term, the first organisation would no longer enjoy a competitive edge and might, ultimately, cease to exist. Both data theft and physical theft can take a number of different forms. As an example, there has been growing concern over the theft of customer information, such as credit card details, from company web sites.

10.1.6 Unauthorised use

One of the most common security risks in relation to computerised information systems is the danger of unauthorised access to confidential data. Contrary to the popular belief encouraged by the media, the risk of hackers, gaining access to a corporate information system is relatively small. Most security breaches involving confidential data can be attributed to the employees of the organisation. In many cases, breaches are accidental in that employees are unaware that particular sets of information are restricted. Deliberate breaches are typically the result of an employee's wishing to gain some personal benefit from using the information obtained. However, we must consider that the threat posed by hackers is starting to increase as more organisations make use of the Internet for business purposes. In addition, it should be noted that even a relatively small number of hacking incidents can account for significant losses to industry.

A hacker is a person who attempts to gain unauthorised access to a computer-based information system, usually via a telecommunications link. However, this is the popular use of this term and is considered incorrect by many IT professionals. Traditionally, 'hacking' referred to the process of writing program code, so hackers were nothing more than skilled computer programmers. Even today, many people consider themselves to be 'hackers' of the traditional kind and dislike being associated with the stereotype of a computer criminal. Furthermore, many people draw distinctions between those who attempt to gain unauthorised access to computer-based information systems for malicious reasons and those with other motivations. A person who gains access to an information system for malicious reasons is often termed a cracker rather than a hacker. Similarly, many people claim to use hacking for ethical purposes, such as helping companies to identify security flaws or assisting law enforcement agencies in apprehending criminals. In general, most people consider hackers to fall into one of three categories of those who wish to demonstrate their computer skills by outwitting the designers of a particular system, those who wish to gain some form of benefit (usually financial) by stealing, altering or deleting confidential information and those who wish to cause malicious damage to an information system, perhaps as an act of revenge against a former employer. Understandably, the most common crime committed by hackers involves telecommunications fraud. Clearly, the first task carried out by most hackers is to obtain free telephone calls, so that the time-consuming task of breaking into a given system can be carried out without incurring a great deal of expense. However, the growth of digital communications technology means that it is possible to implement countermeasures against hacking.

10.1.7 Computer viruses

There are several different types of computer virus. Some examples include:

- The *link virus* attaches itself to the directory structure of a disk. In this way, the virus is able to manipulate file and directory information. Link viruses can be difficult to remove since they become embedded within the affected data. Often, attempts to remove the virus can result in the loss of the data concerned.

- *Parasitic viruses* insert copies of themselves into legitimate programs, such as operating system files, often making little effort to disguise their presence. In this way, each time the program file is run, so too is the virus. Additionally, the majority of viruses are created as terminate and stay resident (TSR) programs. Once activated, the virus remains in the computer's memory performing various operations in the background. Such operations might range from creating additional copies of itself to deleting files on a hard disk.

- *Macro viruses* are created using the high-level programming languages found in e-mail packages, web browsers and applications software, such as word processors. Technically, such viruses are extremely crude but are capable of causing a great deal of damage.

With the possible exception of anti-viruses (described in more detail later), all viruses must be considered to be harmful. Even if a virus program does nothing more than reproduce itself, it may still cause system crashes and data loss. In many cases, the damage caused by a computer virus might be accidental, arising merely as the result of poor programming. There is also evidence to suggest that viruses may be capable of causing physical damage to hardware components. It is possible, for example, to construct a virus that instructs a disk controller to attempt to read a non-existent track, causing immediate and irreparable damage to the hard disk drive. Until quite recently, it was thought that computer viruses could not be attached to data files, such as word processing documents or e-mail messages. However, the built-in programming languages featured within many modern applications mean that data files may now be used to transmit viruses. However, it remains true that viruses cannot be transmitted by a conventional e-mail message. A virus can only be transmitted as an attachment to a message, or if the e-mail package being used allows active content. Two other kinds of programs are related to computer viruses; worms and Trojans. A worm is a small program that moves through a computer system randomly changing or overwriting pieces of data as it moves. A Trojan appears as a legitimate program in order to gain access to a computer system. Trojans are often used as delivery systems for computer viruses.

10.2 Reducing the Threat to Information Systems

In general, there are four major approaches that can be taken to ensure the integrity of an information system. These are containment, deterrence, obfuscation and recovery. Although each strategy is discussed separately, it is important to note that an effective security policy will draw upon a variety of concepts and techniques.

10.2.1 Containment

The strategy of containment attempts to control access to an information system. One approach involves making potential targets as unattractive as possible. This can be achieved in several ways but a common method involves creating the impression that the target information system contains data of little or no value. It would be pointless, for example, attempting to steal data that had been encrypted the data would effectively be useless to anyone except the owner. A second technique involves creating an effective series of defences against potential threats. If the expense, time and effort required to gain access to the information system is greater than any benefits derived from gaining access, then intrusion becomes less likely. However, defences must be continually improved and upgraded in order to keep up with advances in technology and the increasing sophistication of hackers. Thus, such as approach tends to be expensive in terms of organisational resources. A third approach involves removing the target information system from potential threats. Typical ways in which this might be achieved include distributing assets across a large geographical area, distributing important data across the entire organisation or isolating important systems.

10.2.2 Deterrence

A strategy based upon deterrence uses 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. A common method involves constantly advertising and reinforcing the penalties for unauthorised access. It is not uncommon, for example, to dismiss an employee for gaining access to confidential data. Similarly, it is not uncommon for organisations to bring private prosecutions against those who have caused damage or loss to important information systems. Attempts to breach the security of the information system are discouraged by publicising successful actions against employees or other parties. A second approach involves attempting to detect potential threats as early as possible, for example by monitoring patterns of information system usage and investigating all anomalies. However, although such a technique can prevent some attacks and reduce the damage caused by others, it can be expensive in terms of organisational resources. The third technique used commonly involves predicting likely areas of attack and then implementing appropriate defences or countermeasures. If an organisation feels, for example, that it is particularly vulnerable to computer viruses, it might install virus scanning software across the entire organisation.

10.2.3 Obfuscation

Obfuscation concerns itself with hiding or distributing assets so that any damage caused can be limited. One means by which such a strategy can be implemented is by monitoring all of the organisation's activities, not just those related to the use of its information systems. This provides a more comprehensive approach to security than containment or deterrence since it also provides a measure of protection against theft and other threats. A second method involves carrying out regular audits of data, hardware, software and security measures. In this way, the organisation has a more complete overview of its information systems and can assess threats more accurately. A regular software audit, for example, might result in a reduction in the use of illegal software. In turn, this might reduce the number of virus infections suffered by the organisation, avoid potential litigation with software companies and detect illegal or unauthorised use of programs and data.

The dispersal of assets across several locations can be used to discourage potential intruders and can also limit the damage caused by a successful attack. The use of other techniques, such as backup procedures, can be used to reduce any threats further.

10.2.4 Recovery

A strategy based upon recovery recognises that, no matter how well defended, a breach in the security of an information system will eventually occur. Such a strategy is largely concerned with ensuring that the normal operation of the information system is restored as quickly as possible, with as little disruption to the organisation as possible. The most important aspect of a strategy based upon recovery involves careful organisational planning. The development of emergency procedures that deal with a number of contingencies is essential if a successful recovery is to take place. In anticipating damage or loss, a great deal of emphasis is placed upon backup procedures and recovery measures. In large organisations, a backup site might be created, so that data processing can be switched to a secondary site immediately in the event of an emergency. Smaller organisations might make use of other measures, such as RAID facilities or data warehousing services.

10.3 Types of controls

There are five major categories of controls that can be applied to information systems. These are: physical protection, biometric controls, telecommunications controls, failure controls and auditing.

10.3.1 Physical protection

Physical protection involves the use of physical barriers intended to protect against theft and unauthorised access. The reasoning behind such an approach is extremely simple: if access to rooms and equipment is restricted, risks of theft and vandalism are reduced. Furthermore, by preventing access to equipment, it is less likely that an unauthorised user can gain access to confidential information. Locks, barriers and security chains are examples of this form of control.

10.3.2 Biometric controls

These controls make use of the unique characteristics of individuals in order to restrict access to sensitive information or equipment. Scanners that check fingerprints, voice prints or even retinal patterns are examples of biometric controls. Until relatively recently, the expense associated with biometric control systems placed them out of reach of all but the largest organisations. In addition, many organisations held reservations concerning the accuracy of the recognition methods used to identify specific individuals. However, with the introduction of more sophisticated hardware and software, both of these problems have been largely resolved. Many organisations have now begun to look at ways in which biometric control systems can be used to reduce instances of fraud.

10.3.3 Telecommunications controls

These controls help to verify the identity of a particular user. Common types of communications controls include passwords and user validation routines.

10.3.4 Failure controls

Failure controls attempt to limit or avoid damage caused by the failure of an information system. Typical examples include recovery procedures and regular backups of data. Backups are explained in more detail later on.

10.3.5 Auditing

Auditing involves taking stock of procedures, hardware, software and data at regular intervals.

With regard to software and data, audits can be carried out automatically with an appropriate program. Auditing software works by scanning the hard disk drives of any computers, terminals and servers attached to a network system. As each hard disk drive is scanned, the names of any programs found are added to a log. This log can then be compared to a list of the programs that are legitimately owned by the organisation. Since the log contains information concerning the whereabouts of each program found, it is relatively simple to determine the location of any unauthorised programs. In many organisations, auditing programs are also used to keep track of software licences and allow companies to ensure that they are operating within the terms of their licence agreements.

10.3.6 Detecting and preventing virus infection

The risk of virus infection can be reduced to a minimum by implementing a relatively simple set of security measures:

- unauthorised access to machines and software should be restricted as far as possible;
- machines and software should be checked regularly with a virus detection program;
- all new disks and any software originating from an outside source should be checked with a virus detection program before use;
- floppy disks should be kept write-protected whenever possible since it is physically impossible for a virus to copy itself to a write-protected disk;
- regular backups of data and program files must be made in order to minimise the damage caused if a virus infects the system.

Virus scanners are intended to detect and then safely remove virus programs from a computer system. The most common method of detection used by these programs involves scanning for the signatures of particular viruses. It is often possible to locate a virus by simply searching every file on an infected disk for these identifying characteristics. However, since new viruses are discovered quite frequently, the list of signatures contained within a detection program quickly becomes dated. For this reason, most software developers insist that regular program updates are essential. However, the introduction of new kinds of viruses, such as polymorphic and stealth viruses, mean that signature checking alone can no longer be regarded as a completely secure method of detection. For this reason, most virus scanners use a combination of techniques to enhance their efficiency. Amongst the methods used are checksums, virus shields, anti-viruses, heuristics and inoculation. Virus shields are TSR programs that constantly monitor and control access to a system's storage devices. Any unusual attempt to modify a file or write to a disk drive will activate a message asking the user to authorise the operation. A similar task is performed by hardware virus detection devices. Modern hardware protection devices can be extremely sophisticated, featuring their own processors, disk controllers and other expensive components. However, despite the claims of the manufacturers of these devices, there is little evidence to suggest that they are any more effective than software solutions. Once a virus has been detected there are three methods of removing it. The first, disinfection, attempts to restore damaged files and directory structures to their original condition. However, disinfection is not possible in all cases. The second technique involves overwriting the virus program so that it is permanently and irrevocably deleted from the disk. The third and final method of removing a virus is by restoring a backup of the infected disk to the system. The process of writing files to the disk effectively overwrites the virus and restores the system to its original state. Despite the sophistication of scanning programs, none is capable of offering complete protection against infection. Many tests have been carried out to determine the efficiency of specific virus-scanning programs. In all of these tests, no program has yet achieved a perfect score.

10.4 Techniques for controlling information systems

Some of the most common techniques used to control computer-based information systems are:

formal security policies, passwords, file encryption, organisational procedures governing the use of computer-based information systems, user validation techniques and backup procedures. The following describes each of these techniques in more detail.

10.4.1 Formal security policy

Perhaps the simplest and most effective control is the formulation of a comprehensive policy on security. Amongst a wide variety of items, such a policy will outline what is considered to be acceptable use of the information system, what is considered unacceptable use of the information system, the sanctions available in the event that an employee does not comply with the security policy and the details of the controls in place, including their form and function and plans for developing these further. Once a policy has been formulated, it must be publicised in order for it to become effective. In addition, the support of management is essential in order to ensure that employees adhere to the guidelines contained within the policy.

10.4.2 Passwords

The password represents one of the most common forms of protection for computer-based information systems. In addition to providing a simple, inexpensive means of restricting access to equipment and sensitive data, passwords also provide a number of other benefits. Amongst these are that 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. Also the actions of an employee can be regulated and supervised by monitoring the use of their password. Finally 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.

10.4.3 Encryption

An additional layer of protection for sensitive data can be provided by making use of encryption techniques. Modern encryption methods rely upon the use of one or more keys. Without the correct key, any encrypted data is meaningless and therefore of no value to a potential thief.

10.4.4 Organisational Procedures

Under normal circumstances, a set of procedures for the use of an information system will arise from the creation of a formal security policy. Such procedures should describe in detail the correct operation of the system and responsibilities of users. Additionally, the procedures should highlight issues related to security, should explain some of the reasoning behind them and should also describe the penalties for failing to comply with instructions.

10.4.5 User validation

Of relevance to telecommunications is the use of user validation techniques. It is necessary to verify the identity of users attempting to access the system from outside of the organisation. A password is insufficient to identify the user since it might have been stolen or accidentally revealed to others. However, by asking for a date of birth or other personal information, the identity of the user can be confirmed. Alternatively, if the location of the user is known, the system can attempt to call the user back at their current location. If the user is genuine, the call will be connected correctly and the user can then access the system. Although such methods do not offer total security, the risk of unauthorised access can be reduced dramatically.

10.4.6 Backup procedures

The effects of a sudden loss of data can affect a company's activities in a variety of ways. The disruption caused to a company's normal activities can result in significant financial losses due to factors such as lost opportunities, additional trading expenses and customer dissatisfaction.

The cumulative effects of data loss can prove detrimental to areas as diverse as corporate image and staff morale. Perhaps the single most compelling reason for introducing effective backup procedures is simply the expense involved in reconstructing lost data. One of the most common methods of protecting valuable data is to use the 'grand-father, father, son' technique. Here, a rotating set of backup disks or tapes are used so that three different versions of the same data are held at any one time. To illustrate this method, imagine a single user working with a personal computer and using three floppy disks to store their data on. Each day, all of the data being worked on is copied onto the disk containing the oldest version ('grandfather') of that data. This creates a continuous cycle that ensures that the oldest backup copy is never more than three days old. It is worth noting several general points concerning backups of data:

- The time, effort and expense involved in producing backup copies will be wasted unless they are made at regular intervals. How often backups are made depends largely upon the amount of work processed over a given period of time. In general, backups will be made more frequently as the number of transactions carried out each day increases.

- Backup copies of data should be checked each time they are produced. Faulty storage devices and media may sometimes result in incomplete or garbled copies of data. In addition, precautions should be taken against computer viruses, in order to prevent damage to the data stored.

- The security of backup copies should be ensured by storing them in a safe location. Typically, an organisation will produce two sets of backup copies; one to be stored at the company premises, the other to be taken off the premises and stored at a separate location. In this way, a major accident, such as a fire at the company premises, will not result in the total destruction of the organisation's data.

It is worth noting that not all data need be backed up at regular intervals. Software applications, for example, can normally be restored quickly and easily from the original media. In a similar way, if a backup has already been made of a given item of data, the production of additional copies may not be necessary. In order to reduce the time taken to create backup copies, many organisations make use of software that allows the production of incremental backups. Initially, a backup copy of all data files is made and care is taken to ensure the accuracy of the copy. This initial, complete backup is normally referred to as a full backup (sometimes also known as an archival backup). From this point on, specialised backup software is used to detect and copy only those files that have changed in some way since the last backup was made. In the event of data loss, damaged files can be replaced by restoring the full backup first, followed by the incremental backups. One of the chief advantages of creating incremental backups is that it is possible to trace the changes made to data files over time. In this way, any version of a given file can be located and restored.

10.5 Security Threats to Internet services

A number of significant new threats to organisational information systems have emerged connected to the increasing reliance on intranets and the Internet as basic tools for conducting transactions with partners, suppliers and customers. Although the following material focuses on the Internet, much of it is also relevant to company intranets.

10.5.1 Denial of service (DoS)

As companies begin to rely on network technology to reduce costs, they become more vulnerable to certain risks. For example, more harm can be caused if an individual gains access to a network server than if they merely gain access to a single PC. Similarly, companies relying on the Internet for business communications may find themselves subject to denial of service attacks. Typically, these attacks involve blocking the communications channels used by a company. For example, an e-mail system might be attacked by sending millions of lengthy messages to the company. Other techniques involve altering company web pages or attacking the systems used to process online transactions. In these cases, companies are usually forced to shut down services themselves until the problem can be dealt with. The impact of a denial of service attack can be extremely severe, especially for organisations that rely heavily on the Internet for e-commerce.

10.5.2 Trojans

Recently the use of Trojans to disrupt company activities or gain access to confidential information has grown sharply. Most of the Trojans encountered by business organisations are designed to gather information and transmit regular reports back to the owner. Typically, a Trojan will incorporate a key logging facility (sometimes called a ‘keystroke recorder’) to capture all keyboard input from a given computer. Capturing keyboard data allows the owner of the Trojan to gather a great deal of information, such as passwords and the contents of all outgoing e-mail messages. Some Trojans are designed to give owners control over the target computer system. Effectively, the Trojan acts as a remote control application, allowing the owner to carry out actions on the target computer as if they were sitting in front of it. Sometimes, the owner of the Trojan will make no effort to conceal their activities: the victim sees actions being carried out but is unable to intervene, short of switching off the computer. More often, however, the Trojan operates silently and the victim is unaware that their computer is running programs, deleting files, sending e-mail, and so on. Some programs are designed to disrupt company activities by initiating denial of service attacks or by attacking company servers. However, incidents involving these kinds of Trojan are rare since they often require very high levels of access to company systems.

10.5.3 Identity theft and brand abuse

Identity theft involves using another person's identity to carry out acts that range from sending libellous e-mail to making fraudulent purchases. It is considered relatively easy to impersonate another person in this way, but far harder to prove that communications did not originate from the victim. For business organisations, there is a threat that employees may be impersonated in order to place fraudulent orders. Alternatively, a company may be embarrassed if rumours or bogus press releases are transmitted via the Internet. The term brand abuse is used to cover a wide range of activities, ranging from the sale of counterfeit goods, for example software applications, to exploiting a well-known brand name for commercial gain. As an example, the name of a well-known company might be embedded into a special web page so that the page receives a high ranking in a search engine. Users searching for the name of the company are then likely to be diverted to the special web page where they are offered a competitor's goods instead.

10.5.4 Extortion

Various approaches can be used to extort money from companies such as cybersquatting and the threat of divulging customer information. Cybersquatting involves registering an Internet domain that a company or celebrity is likely to want to own. Although merely registering a domain is not illegal in itself, some individuals attempt to extort money from companies or celebrities in various ways. Typically, the owner of the domain will ask for a large sum in order to transfer the domain to the interested party. Sometimes, however, demands for money may be accompanied by threats, such as the threat the domain will be used in a way that will harm the victim's reputation unless payment is forthcoming. Although there is an established mechanism for dealing with disputes over domain names, many victims of cybersquatting choose not to use these procedures since they do not wish to attract negative publicity. A more common form of extortion usually occurs after a security breach in which sensitive company information has been obtained. Often, the threat involves making the information available to competitors or the public unless payment is made.

10.5.5 Abuse of resources

Organisations have always needed to ensure that employees do not take advantage of company resources for personal reasons. Whilst certain acts, such as sending the occasional personal e-mail, are tolerated by most companies, the increased availability of Internet access and e-mail facilities increases the risk that such facilities may be abused. Two examples of the risks associated with increased access to the Internet involve libel and cyberstalking. Cyberstalking is a relatively new form of crime that involves the harassment of individuals via e-mail and the Internet. Of interest to business organisations is the fact that many stalkers make use of company facilities in order to carry out their activities. There have also been cases of 'corporate stalking' where an organisation has used its resources to harass individuals or business competitors. For an organisation, the consequences of cyberstalking can include a loss of reputation and the threat of criminal and civil legal action.

10.5.6 Other risks

This section provides a discussion of two additional examples of emerging threats: cyberterrorism and stock fraud. Cyberterrorism describes attacks made on information systems that are motivated by political or religious beliefs. Organisations involved in the defence industries are often the victims of such attacks. However, many other companies are also at risk from politically motivated attacks. For example, companies trading in countries that are in political turmoil or companies with business partners in these countries also face the risk of such attacks. A number of recent cases have highlighted the danger of allowing inaccurate or misleading information to propagate across the Internet. Online stock fraud involves artificially increasing or decreasing the values of stocks by spreading carefully designed rumours across bulletin boards and chat-rooms. Whilst such activities may seem relatively harmless, companies can suffer significant losses. Incidences of online stock fraud highlight an extremely important issue: organisations are at risk from the distribution of false information across the Internet. It is important to note that the effects of online stock fraud are not limited only to influencing stock prices. Imagine, for example, what might happen if bogus press releases began to appear when a company was in the process of negotiating a merger or strategic alliance. Preventing inaccurate or misleading information from appearing on the Internet is fraught with difficulty. The sheer size of the Internet means that monitoring web sites, chat-rooms and news services places an unacceptable burden on the resources of even the largest organisations.