

## Computer security

Computer security is concerned with taking care of hardware, software and most importantly, data. The cost of creating data again from scratch can far outweigh the cost of any hardware or programs lost. Loss of data can have various consequences, some of which are shown in Figure 16.1.

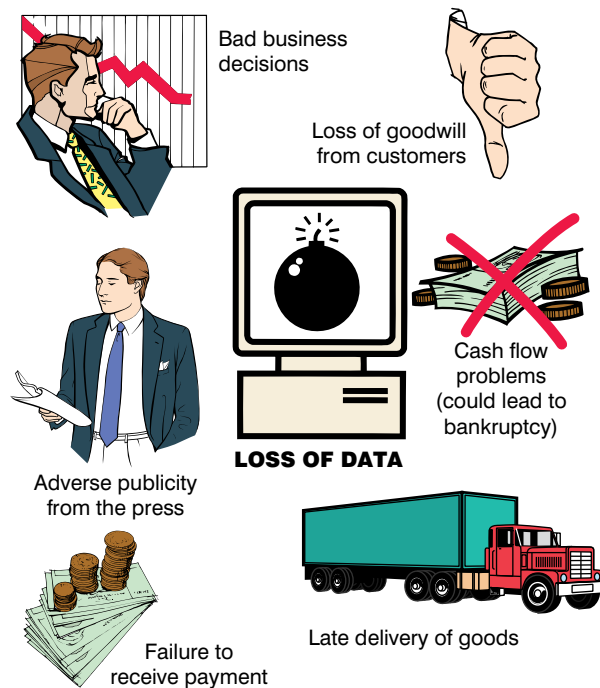


Figure 16.1 Some of the consequences of data loss

## Physical security

Computer equipment and its data need to be protected from physical harm. Hazards could include natural ones such as fire, lightning, water damage, etc., and can also include deliberate damage or theft.

## Computer theft

Although there are many ways of making sure that unauthorised people are denied access to

a system through the use of keyboard locks, passwords, etc., it is more difficult to prevent a thief from picking up a system and stealing it. Locks, bolts, clamps, alarmed circuits and tags are all methods of hardware protection. Although not many people would consider leaving a bicycle without a lock, people do often leave thousands of pounds worth of computer equipment unlocked and unattended.

Sometimes it is easier to improve the security around a computer system. Usually, if a building is secure, the computer system will be secure.

Having fewer entrances to buildings, using alarms on emergency exits, using security badges and having keypad locks on all rooms will all help.

## Preventing computer theft

- 1 A note should be made of all the serial numbers of computers and peripherals, since this may be the only way that the police can identify stolen equipment.
- 2 It is possible with some computers to lock the case of the computer, which prevents the computer from being turned on. This should always be done when the computer is not in use and the key should be safely stored in a secret place and not in the top drawer of the desk that the computer stands on.
- 3 Data should be backed up regularly and stored securely away from the computer. If the computer system is stolen then at least the data, which would be a lot more expensive to recreate, is safe.
- 4 All staff should be made aware of security and encouraged to question suspicious behaviour.
- 5 If an ID badge system is used (where staff and visitors have to wear a security badge which contains their photograph, name,

etc.) then everyone from the chairman to the cleaners must wear them since this indicates to outsiders that the firm is security conscious.

## Protection from fires

Fires which start in computer rooms are rare. Usually they are the result of faulty wiring or overloaded sockets. It is more likely that a fire will start in adjacent offices or in storage areas. Fireproof doors help contain fires. Smoke detectors should be used to detect fires at an early stage. Gas flooding systems are used in large computer installations and are preferred to water ones because the damage done by water is often greater than that by the fire.

## Protection from dust and extremes of temperature

Air conditioning is more important for larger mainframe systems where the temperature and the humidity (amount of water in the air) must be controlled. The air must also be pure and is therefore filtered before it enters the room.

## Software security

### Viruses

Viruses are mischievous programs the purpose of which is to disrupt the sensible use of computers. Many viruses do little more than display a message (usually insulting!) on the screen, but some are designed to act after a certain period of time and do such things as make the letters start to drop off the screen or even erase the entire contents of your hard disk. As their name suggests, viruses are able to spread by 'infecting' other disks and they do this by copying themselves onto other disks which are being used by the computer. Although there are many viruses (over 2000 to date), the main problems are caused by a handful of very familiar ones with names such as: Cascade, Form, Jerusalem and Stoned.

Since these viruses have been around for some time, they are well understood and easy to remove from computers by anti-virus software. Viruses are quite common, especially in situations where there is a large number of users such as in a school or college.

### Antivirus software

Antivirus software can be used to scan a computer's memory and disks to detect viruses. Any viruses detected are then removed using the software (disinfecting a disk, as it is often called). When choosing antivirus software, speed of checking is important.



Figure 16.2

### Avoiding viruses

- 1 Don't buy secondhand software unless you can scan it first.
- 2 Check your computer for viruses if it has been recently repaired.
- 3 Do not download software from bulletin boards, since this is the easiest way for the people who produce viruses to distribute their handiwork.
- 4 Be suspicious of all software distributed freely, such as shareware and software which comes free with magazines as these have sometimes had viruses on them.

- 5 Try not to use too many different computers, since this will increase the risk of passing on a virus.
- 6 On your own machine, install anti-virus software which checks for viruses on the hard disks every time the system is booted up and checks all floppy disks before data is taken from them.
- 2 If you hold a lot of data which would be very expensive to recreate, then you should invest in a fire-proof safe to protect your backups against theft and fire.
- 3 Keep at least one set of backup disks in a different place (i.e. at a different site).

## Backing up data

Backing up data means taking a copy of the data and keeping it away from the computer in a secure place. Obviously it is no good keeping a backup copy on the same disk.

The most common way to lose a file is through user error, where a person makes a mistake with one of the commands and deletes a file or a whole series of files which they did not intend to delete. Although there are software packages available to recover such data these should not be relied upon and there is no substitute for having a backup copy of the data in a secure place.

### Rules for backing up

- 1 Never keep backup disks near the computer. If the computer is stolen the thieves may take the disks as well. Never keep the disks in the drawer of a desk since this is the first place thieves will look.



Figure 16.3

### Archiving

Archiving means placing important computer files in a safe place so that they can be found easily if needed.

## Disk failure

It is important to bear in mind that all micro-computers will suffer at least one serious fault during their lifetimes. A typical hard disk unit has a mean time between failures of between 20 000 to 200 000 hours. This means that if a computer was used for 12 hours per day, 5 days per week and 52 weeks a year then you could expect its hard disk to break down once in about six years. If the computer is being used as a file server (i.e. used to control a network) it could be switched on 24 hours per day 365 days per year, so the hard disk would fail on average every 27 months. Couple this with the chance of other components failing and you have a complete computer which is likely to break down every 14 months.

Backup copies of the programs and data on a hard disk should be taken at regular intervals. A tape streamer is usually used. This looks a little like an ordinary tape recorder. Transfer from the hard disk to the tape takes place quickly and you don't have to supervise the computer while backup is taking place. Should the hard disk become damaged, then it is easy to restore files.

Figure 16.4 shows some of the security features of a 3.5 inch floppy disk.

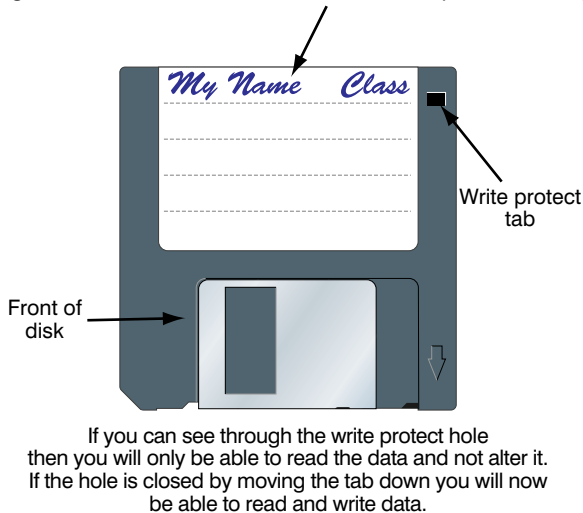
Some systems use two hard disks in parallel with each other, which means that whatever is stored on one disk will be stored automatically on the other.

## Protecting your files

Software can be written which does not allow access to a computer unless a password is keyed in. The password, which is never

shown on the screen, should be changed regularly and should never be written down. Obvious names, such as the surname of the person using the machine, should be avoided, along with other obvious passwords such as 'access'.

Always write where the disk should be returned if lost (e.g. name and address of home or school or a phone number)



**Figure 16.4** Some of the security features on a 3.5 in disk

Many large systems use software to limit each user's access to only those files that are needed for the performance of their particular job. So, for instance, an accounts clerk could have a password that allows access to files needed for checking invoices, whereas the accountant would have access to all the accounts files.

It is also important to try to restrict access to a computer's operating system particularly for inexperienced users. A simple command at the operating systems prompt can erase an entire hard disk. Restricted access can also be used to prevent people from copying data from the hard disk to a floppy disk.

## Encryption

Sometimes files which contain sensitive data are encrypted (i.e. coded). If a tape or disk containing sensitive files is stolen it would then be impossible to read the data without the decoder.

Encryption is often used when important data is transmitted from one place to another.

The data is coded before being sent and then decoded at the other end. Both processes are performed automatically by computers. Should the data be intercepted, then it will be impossible to understand or alter. When people are making payments for goods bought over the Internet using a credit or debit card the details are always encrypted.

## Project advice

Always keep backup copies of your work and don't keep your backups in the same disk box as your original disks.

If a disk becomes corrupted for whatever reason and you haven't taken a backup don't immediately throw the disk away. There are various programs that are able to recover data from corrupted disks. Norton Utilities is one such package. If you do have a corrupted disk ask your teacher to use one of these packages to look at the disk and if it is possible to recover any of the data.

If you have accidentally deleted a file that you wanted to keep, tell your teacher. Again, using special software it is possible to get the file back.

## The difference between security and integrity

### Data integrity

Data integrity is concerned with the 'correctness' of the data. Errors may be introduced into data in a variety of ways. They can be introduced when the person typing in the data misreads it off a source document or if a program or machine errors corrupt the data. Some types of corruption can be caused by simple typing errors. Validation and verification checks are performed on data to ensure its integrity and further information about this can be found in Chapter 7.

### Data security

Data security is concerned with keeping the data safe from the various hazards that could destroy it.