PC Passport

IT Security
Student Workbook

Published date: August 2008

Publication code: CB4125

Published by the Scottish Qualifications Authority
The Optima Building, 58 Robertson Street, Glasgow G2 8DQ
Ironmills Road, Dalkeith, Midlothian EH22 1LE

www.sqa.org.uk

Introduction

This student workbook is one of a range of eight titles designed to cover topics for the refreshed PC Passport. Each title in the range covers the required subject material and exercises for candidates studying PC Passport.

This workbook covers PC Passport Advanced: IT Security for Users.

There are a number of exercises associated with each subject and it is recommended that centres download and use the sample exercise files provided.

Each workbook will help prepare candidates for the assessments for the refreshed PC Passport. It is recommended that centres use the most up-to-date Assessment Support Packs appropriate for their type of centre, eg either school, FE or work-based.

Contents

Computer Security

Computer security is concerned with taking care of hardware, software and most importantly the data contained within a computer system. If the data is destroyed, lost or compromised 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, depending upon the amount and type of data lost.

There are five main areas that need to be considered when looking at computer security:

1. implementation of physical security
2. protection from environmental disasters
3. protection from software issues
4. protection from hardware failures
5. protection from human failures.

Physical Security

Computer equipment and its data need to be protected from physical harm. Hazards that need to be considered could include the natural ones such as fire, lightning, water damage, etc, and can also include deliberate damage to hardware or the theft of the computer system or parts of the computer system.

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 that are utilised within an organisation.

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.

It is sometimes easier to improve the security around a computer system rather than try to secure each individual computer system. Usually, if a building is secure, the computer systems within will also 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, and department then it is difficult for a thief to enter a building without someone questioning the lack of identification.

Environmental Disasters

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 another part of the building or in a storage area. Fireproof doors will help contain fires and smoke detectors should be used to detect fires at an early stage. Gas flooding systems are used in computer rooms in preference to water sprinklers because the damage done by water to a computer system is often greater than the damage caused by a fire. The physical machine may be destroyed but the hard drives etc may be readable and the data retrieved.

Protection from Dust and the Extremes of Temperature

Air conditioning is more important for the 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 Failure

Virus

A *virus* is a program which can reproduce itself. A virus on a hard disk of an infected computer can reproduce itself on to a floppy disk or memory stick. When the floppy disk or memory stick is used on a second computer, the virus copies itself on to this computer's hard disk. This copying is hidden and automatic and the user usually is unaware of the existence of the virus — until something goes wrong. Viruses are written to either disrupt or take control of other users’ computers.

Virus programs are becoming more and more sophisticated as the makers move to other methods of propagation. The internet has made the delivery of this type of program more problematic as the move away from floppy disk drives continues.

Viruses are delivered in a variety of ways including accessing websites, e-mail, picture files, application macros etc. Thousands of viruses exist with damage varying from the trivial to the disastrous.

Viruses can be prevented by not allowing users to bring their removable storage devices to use on the system, or to take the company's disks home to use on their own PC. Systems can be set up only to allow specially formatted disks, so that users cannot use their home computer disks.

Viruses can also be controlled by restricting access to the Internet, however this has many problems, as most web marshal systems look for specific words on a web page and if found the page is blocked. Sometimes you can find access to a website blocked even if you require access because for your work, for example most web marshal systems do not allow employees to download zipped files from website, even if it’s the company’s own website, which restricts an employees legitimate ability to access company information.

Viruses can be detected and damage repaired using *anti-virus toolkit* software. This sort of software is widely available and can detect and repair thousands of viruses. Whenever an infected device is placed in the computer's drive, a warning message appears on the screen. Updates of this software are produced every day (sometimes every few hours) as new viruses are detected. Most virus software packages will update the virus definition files when they are connected to the internet automatically.

Software Security Viruses

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, steal passwords or credit card details, or 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. You can read more about viruses in the PC Passport Internet & On-line Communications Unit.

Although there are many viruses (over 200,000 to date), the main problems are caused by very familiar ones which tend to target flaws within the operating system. This means the some operating systems are attacked more than other similar systems.

Since most of the 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 are a large number of users such as in a school, college or university.

Anti-virus software can be used to scan the computer's memory and disks to detect viruses. Any viruses detected are then removed using the software.

How to Avoid Viruses

1 Do not buy second-hand software unless you can scan it first.

2 Set up your machine to automatically scan all removable devices that are connected to your computer system.

3 Check your computer for viruses if it has been recently repaired.

4 Do not download software from unreliable sources, since this is the easiest way for the people who produce viruses to distribute their handiwork. Examples of this are Warz sites, Kezza sites etc.

5 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.

6 If you must download software from these sources then check for viruses using a virus checking program before you run or try to install them.

7 Try not to use too many different computers, since this will increase the risk of passing on a virus.

8 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 or memory sticks before data is taken from them.

Hardware Failure

It is important to bear in mind that a microcomputer is likely to suffer at least one serious failure during its lifetime. A typical hard disk has an average time of failure 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 system is continually switched off and on then this time period is reduced as there is more wear and tear on the starting up and stopping process. If the computer is being used as a file server (ie used on a computer 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.

Add this to the other components that fail in your computer system and you have a complete computer system which is likely to break down every 14 months.

Human Failures

The most vexing weakness in any computer security system is not in the hardware or the software; it is in the people who use the actual machines. This is according to top hackers and system safety specialists. Poor security is really more of a human problem than a technical problem.

Some examples of this are users who routinely leave passwords on Post-it notes taped to machines or under keyboards and share supposedly secret access codes with their co-workers. There is a chance that if you asked someone in your office for their computer password they would give it to you. A well known fact is that this password once given will probably let you into their e-mail account, bank account etc. A large number of people have one password that they use for everything.

Other identified problems are people that use the simplest of passwords to protect systems — for example initials, age, etc. These passwords can be broken by password cracking software in a matter of seconds.

The internet is awash with bogus *phishing* e-mails written by fraudsters. A phishing e-mail might look as if it comes from your Technical Support Department — but asks for your password details. Understandably, people will not give out bank details, but a password? No problem!

Last, but not least, users need training in the correct use of the computer system(s) that they are using. Untrained users can intentionally or unintentionally subvert security policies through lack of training.

Solutions to these problems do exist and policies can be put in place to stop simple passwords, etc but it is more difficult to stop people writing down their passwords.

Backing-up data

Backing-up — Backing-up data is the name given to the process of making a copy of data stored on the computer system's hard disk drives, be it to digital magnetic tape or other portable media. The only purpose of backing-up data is to ensure that the most recent copy of the data can be recovered and restored in the event of data loss.

Archiving — Archiving data is the name given to the process of copying data from hard disk drives to tape or other media for long-term storage. This is generally used to free hard disk space by off-loading seldom used data to tape.

Disaster recovery — Archived data can be used to recover from disasters such as fires or floods, where data stored on primary devices is destroyed. In a well-planned scheme, a copy of the business data is delivered to a secure offsite storage facility. A rotation system can provide data version history, depending on the needs of the business and the criticalness of the data.

Storage methods — Although most business data is stored on hard disk, some data such as customer records can be stored on tape. Using digital magnetic tape has many benefits including cost savings. However a high data transfer rate is essential for maintaining productivity.

The longer the organisation keeps its data, the more portable media are needed to store the data. When determining how long your data must be retained, you must consider any legal obligations for your type of business as well as all other business needs. If your data needs to be stored for a long time, you need to frequently inspect the media for signs of damage.

The Process

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.

There are three main types of backup that need to be considered. The amount of data stored in each backup is different for each strategy. Also, what you are including in the backup needs to be considered. Are you backing-up the complete computer system contents, programs, operating system and data or are you concerned only with the data? This choice obviously makes a difference to the amount of data being stored and also the time taken to perform the backup.

Full Backup

A *full backup* is a complete backup of all the files on the system being backed up. When you perform an initial backup of your computer system this strategy should be adopted.

You can then move to one of the other strategies depending upon your preference. This guarantees that a complete restore can be done with only backup session.

The downside is that it takes longer backup times each day. This type of backup is common for smaller servers with less than 1 gigabyte of data and which do not need to be up 24 hours a day for operation.

Differential Backup

A *differential backup* involves only the files that have changed since the last full backup. This is a variation of the above method where one backup session contains a full image of the computer system data and subsequent backup sessions only copy files which are different or were updated after the initial backup. This allows the complete computer system to be restored with a maximum of just two backup sessions should a full system restore be needed.

Modified Backup

A *modified backup* involves only the files that have changed since the last full or differential backup. Using this variation of the differential backup method only the files that have changed since the last backup are stored. This type of backup would take less time to backup each time and could be done several times during the day. It will however require more time to restore since several backup sessions may be required for a total restore.

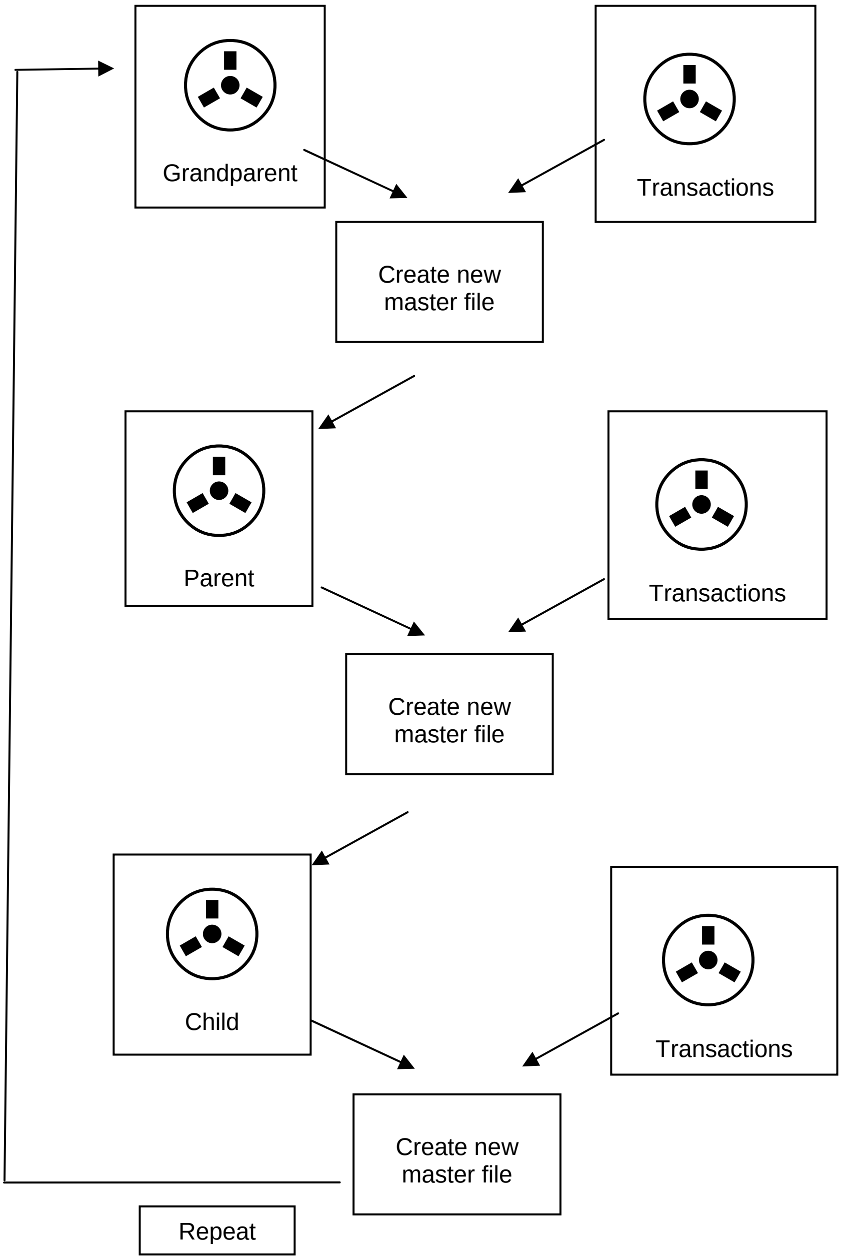
Determine the Frequency of Your Backup

Most of the software solutions for backup offer automated scheduling. Depending on how often you use your PC, scheduling a backup is a great way to provide peace of mind and ensure the safety of your data.

A good management plan is required to ensure the backups are performed at the appropriate intervals. Most organisations backup daily but backups may need to be performed more or less frequently. Whereas an individual may only backup data once a month, once a year or even never. A rotation scheme that provides an appropriate data version history should be selected.

The *grandparent-parent-child* scheme shown below uses tapes to allow recovery of data on a daily, weekly and monthly basis.

Grandparent, Parent, Child Rotation Scheme



Choose Your Backup Medium

You need to decide on the best media type for your backups. This has to be based on how much data you are backing-up, how often your backups are scheduled, and the life of the medium.

For simple file-by-file backups (critical files, such as documents, address book, e-mails), you could choose to backup to an 8 Gb USB memory drive. The USB drive is not only portable it is also rewritable, relatively fast, virtually indestructible, and has a life of about 100+ years. This is a perfect device for retaining small- to medium-sized files. The capacity of these devices is increasing and seems to be doubling almost every 8–10 months at present.

However, if you wish to backup your entire hard drive, other devices need to be considered. What you use depends on the quantity of information stored on your hard drive and the size of the hard drive.

Most computer systems have DVD-RW devices which means that you can backup data to a rewritable DVD disk, these can hold about 4 Gb of data. However, if you have around 700 Gb of data then you would need a considerable number of DVDs for the backup.

For large backups, a tape drive is still an economic device, or perhaps you can backup to another machine across your network. There are various options that need to be considered.

Always Check the Source Data for Errors

Before beginning any backup of data, it is absolutely critical to ensure that the integrity of the data is valid; otherwise, all your backups will be worthless. If you are backing-up data on the hard drive, scan the drive for file system errors.

Rotate Your Backups Whenever Possible

Do not use the same device for your data images. This means you should have a couple of sets of media available; you should rotate your backups onto a different set up medium every 2 weeks. By doing this if one of the sessions develops a fault during a restore you can refer to the previous week's backup session.

Always Test the Integrity of Your Restore

Even though the data is backed up, what guarantee is there that you can restore the data when something goes wrong? All too often, most individuals do not ask this question before it is too late. If the data cannot be restored then you might as well not have performed the backup.

Aside from physically restoring the data back to the hard drive, the best way to ensure the 'restorability' of your data is to use a backup solution that has bit-level verification. This option may be available in your backup software.

Store Copies of the Backups in a Safe Location(s)

Once your backup is complete and data integrity has been checked, you should store your backup in an atmosphere-friendly place. This means a location safe from fire, water, or direct sunlight exposure. For the ultimate backup protection, you should also keep a copy of your backup data in a secure location off-site away from your home or place of work.

For Further Information

The following pages at the Wikipedia site give a good summary of backup procedures http://en.wikipedia.org/wiki/Backup

Protecting Access to Your Data 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'.

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 system’s 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 removable device such as an MP3 player.

Encryption

Sometimes files which contain sensitive data are *encrypted*. If a tape or disk containing sensitive files is stolen it would then be impossible to read the data without knowing the decoding key or having the actual decoder device. Data encryption is often used when important data is transmitted from one place to another across unsecured networks such as the internet.

The data is coded before being sent and then decoded at the other end. Both processes are performed automatically by the computers at either end. Should the data be intercepted, then it will be impossible to understand or alter the contents. When people are making payments for goods bought over the internet using a credit or debit card the details are not always encrypted. In order to confirm that encryption is being used you need to check that the web address begins http**s**:// and that the security padlock is shown onscreen. The connection is then secure and encrypted.

An example of encryption is the banks' Electronic Funds Transfer (EFT) system. Banks and other financial institutions transfer vast sums of money electronically. These transfers are protected by the latest data encryption techniques.

The simplest of all of the methods of encrypting data uses a translation table. Each character is replaced by a code character from the table. However this method is relatively straightforward for code breakers to decipher. More sophisticated methods would use two or more tables.

Even more sophisticated methods exist based on patterns, random numbers and using a key to send data in a different order. Combinations of more than one encryption method make it even more difficult for code breakers to determine how to decipher your encrypted data. Encryption schemes can still be broken, but making them as hard as possible to break is the job of a good cipher designer. However, you should always remember that even the best security may still be broken.

Computers and Privacy

The rapid explosion in the use of computers in the last 15 to 20 years has benefited us in many diverse ways. Many of the everyday uses of things that we now take for granted, such as the use of credit cards and cash dispensers would have been impossible without the development of computer systems. However, there are problems. As computer use increases, more and more information about each of us is being stored on computer systems. Large databases of information are built up and by linking the information gained from several computer systems together it is possible to build up a complete picture of an individual’s life.

Loyalty Cards

Most large store chains have what is called a loyalty card scheme. Each time the customer uses the card, points are added. These are common in supermarkets, music stores etc.

When the number of points earned reaches a certain value customers are given vouchers that can generally be used in the store instead of cash.

The use of these cards is two fold:

1 It makes the customer become loyal to a particular store chain.

2 The scheme can be used to provide useful marketing information about each customer and the items they have purchased.

Before the introduction of loyalty cards, if you paid cash, then the store did not know who you were. They had no way of linking you to any of the purchases you had made. With the loyalty card they can find out lots of useful information about you and what you like to buy, when you like to buy, your taste in music etc.

All this data is stored in electronic form as this makes it easier to process for the organisations. However, it is also much easier to misuse electronic information than information kept in traditional paper form. Documents such as invoices, purchase order etc.

Advantages

1 Cross referencing is easy using a computer to link the data from different systems.

2 Faster access to data. It is much quicker to gain access to electronically held data and copy or print it than it is to search through manually held files.

Disadvantages

1 If the system uses external communication links then there is a risk of people gaining unauthorised access (*hacking*) and looking at, or changing confidential information.

2 When making alterations to data on paper then these can usually be seen. There is no such physical evidence when alterations are made on a computer system.

The Data Protection Act

As more and more information is being stored on computers, much of it personal data about individuals, there became the need for some sort of control over the way that it was collected and the way it could be used. In 1984 an Act of Parliament called The Data Protection Act was passed to deal with the problems of data held on computer systems. The Data Protection Act 1998 subsequently replaced the 1984 Act.

The purpose of the new Act is to deal with some of the things that were not envisaged when the older Act was introduced. These new things include the internet, loyalty cards and the use of huge customer databases for marketing purposes. The new Act also covers manually-held data not covered by the earlier Act.

The revised Data Protection Act 1998 covers the processing of data, either manually or by a computer system.

The Act places obligations on those people who record and process personal data; these people are called the *data controllers* in the Act. Data controllers must be open about their use of the data by telling the *Data Protection Commissioner* (the person who enforces the Act) that they are collecting personal data and how they intend to use it.

They must also follow a set of eight principles, called the *Data Protection Principles.*

The Data Protection Principles

The principles state that:

1 The personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the following conditions are met:

- ♦ The data subject has given their permission for the processing.
- ♦ The processing is necessary for the performance of a contract which involves the data subject.
- ♦ The data controller has a legal obligation to process the data.
- ♦ The processing is necessary to protect the vital interests of the data subject.
- ♦ The processing is necessary for the administration of justice or for a government department.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be adequate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Act mentions data called ‘sensitive personal data’, which may not be disclosed and this includes information about:

- the racial or ethnic origin of the data subject
- their political opinions
- their religious beliefs
- whether or not they are a member of a trade union
- their physical or mental health or condition
- the commission or alleged commission by them of any offence or
- any proceedings for any offence committed or alleged to have been committed by them and if they are convicted, the sentence given.

A data controller means a single person or a group of people who determine the purpose for which, and the manner in which, any personal data is processed. The data controller is therefore the person who decides what to do with the data once it has been entered onto the computer or manual system.

The Data Protection Commissioner (DPC), the person who enforces the Data Protection Act, must be notified by the data controller if they hold data not falling into one of the categories covered by the exemptions.

Registering with the Data Protection Commissioner

So what happens if an organisation doesn't register? If an organisation does not register its use of personal data or it provides false information to the Commissioner, then the organisation may be fined up to £5000 in the magistrates' court or an unlimited fine in the High Court.

Everyone, whether we like it or not is a data subject, this is due to the fact that organisations and companies, called *data users*, will hold personal details about us on their computer systems. The worrying thing about this is that, because of the power of and the ease of communication between computer systems, this data can be transferred from one computer to another at the press of a button. This means that data collected by one computer user can be transferred to other users, who can utilise the information for a completely different purpose. The sale of personal information is becoming big business.

How does this affect you? Well for example, if you own a television set, then your details will be automatically passed to TV Licensing — the TV licence centre. If you own a vehicle then information that you provide to The Driver and Vehicle Licensing Authority (DVLA) is linked to the Police National Computer. Banks and building societies are required by law to automatically notify the Inland Revenue if a person receives over a certain amount of interest in a year.

However, it is not all doom and gloom. The transfer of personal data between computers does have some advantages. For example, without the rapid transfer of records the capture and conviction of criminals would be made more difficult. It makes it easier to tax your vehicle online so there are benefits as well.

However, there are dangers that we should be aware of. Suppose your record gets mixed up with someone else's record or that incorrect data is entered into your record? This could have various results:

- you could be refused credit or benefits or even a job
- in certain cases it could result in you being arrested.

The Data Protection Act gives us the right to see our personal data kept on computer and to get it corrected if it is wrong. It also gives us the right to complain to the Data Protection Commissioner if we do not like the way the data is collected or the way that it is being processed and used.

How Does This Apply to Me?

Not everyone has to register their use of personal data, so, if you hold your address book or your Christmas card list on your home computer, you can sleep at night. There are exemptions to the Act. In other words, you do not need to register your use of personal data if your use falls into any of the following categories:

- When the data held is being used only in connection with personal, family or household affairs, or for recreational use.
- Where the data is being used only for preparing the text of documents.

- Where the data is being used only for the calculation of wages and pensions or for the production of accounts.
- Where the data is used for the distribution of articles or information (eg unsolicited mail, ie mail that advertises goods or services that you have not asked for). This is why junk mail is so difficult to stop.
- Where the data is held by a sports club or a recreational club which is not a limited company.

As a data subject you have the right to see any personal details about you held on computer or held manually. You also have the right to a description of the data being processed. This means if you do not understand what the data means, then you can have it explained. You are also entitled to know the logic behind any decisions made when the decision is made automatically.

To see these details it is necessary to send a letter or e-mail to the organisation concerned. The organisation may ask for a modest fee to cover the expense in providing the information. By law they have 40 days to respond to your request.

You should note that you do not, however, have the right to see all the information held about you. You may be denied access to the information if it is being used for any of the following purposes:

- the prevention or detection of crime
- watching or prosecuting offenders
- collecting taxes or duty (eg VAT)
- medical or social workers' reports in some instances.

Personal data which consists of a confidential reference (for a course or for employment) is exempt from subject access. This means you cannot apply to see your personal reference. Examination scripts and examination marks are also exempt from subject access.

So you cannot demand your exam scripts back or see your exam results before they are formally published.

The Data Protection Act — A Summary

The following are the key point that should be noted in relation to the Act:

- All personal data must be obtained fairly and lawfully. The data subjects need to be informed of whom the data controller is and the purpose or purposes for which the data are intended to be processed. The data subject must also be informed to whom the data will be disclosed. For the majority of students this is done by the collage or university when you sign your registration form. There will generally be a paragraph giving these details.
- The new Act covers personal data in both electronic form and manual form (eg paper files, card indices) if the data is held in a relevant, structured filing system.
- Personal data processing must be in accordance with the purposes notified by the institution to the Data Protection Commissioner. If any 'new processing' is to take place the Data Protection Representative, must be consulted and informed.
- Personal data must be kept accurate and up to date and not be kept for longer than is necessary.
- Appropriate security measures must be taken against unlawful or unauthorised processing of personal data and against accidental loss of, or damage to, personal data. These include both technical measures, eg data encryption and the regular backing-up of data files and organisational measures.
- Personal data shall not be transferred to a country outside the European Economic Area unless specific exemptions apply (eg if the data subject has given consent) this includes the publication of personal data on the internet.

The Rights of the Data Subject

As a data subject certain rights are granted these include the following:

1 To make a subject access request. The individual is entitled to be supplied with a copy of all personal data held. There may be a small nominal fee for this information.

2 To require the data controller to ensure that no significant decisions that affect them are based solely upon an automated decision taking process.

3 To prevent processing likely to cause damage or distress.

4 To prevent processing for the purposes of direct marketing.

5 To take action for compensation if they suffer damage by any contravention of the Act by the data controller.

6 To take action to rectify, block, erase or destroy inaccurate data, and

7 To request the Data Protection Commissioner to make an assessment as to whether any provision of the Act has been contravened.

Further Information

For further detailed information you can consult the following two reference sources:

- ♦ The full contents of the act can be found at Office of Public Sector Information http://www.opsi.gov.uk/acts/acts1998/19980029.htm.
- ♦ A good summary of the act can also be found on the Wikipedia site at http://en.wikipedia.org/wiki/Data_Protection_Act.

The Copyright, Designs and Patents Act

The Copyright, Designs and Patents Act makes it a criminal offence to copy or steal software.

Under the Act it is an offence to copy or distribute software or any manuals which come with it, without permission or a licence from the copyright owner, who is normally the software developer. It is also an offence to run purchased software covered by copyright on two or more machines at the same time, unless the licence specifically allows it.

The Act makes it illegal for an organisation to encourage, allow, compel or pressure its employees to make or distribute copies of illegal software for use by the organisation.

Introduction to the Copyright Laws

Copyright is a set of rights vested in the owner of a protected work. There are various types of work and each type of work has different copyright protection. This probably adds to the confusion on the issue of copyright.

It should be noted that there is no copyright protection for ideas, these are dealt with under the Patents Act and are not discussed in this workbook.

Each type of work has a different status in law, and each may require different strategies and considerations to obtain clearance for use, and the term of copyright in each category can vary.

To qualify for copyright protection, the work must be original, that is, not copied. Copyright is automatic, so once an original work is created, copyright in it exists without the need to register, pay fees or undergo any bureaucratic procedures. Furthermore, copyright is simultaneously created automatically in all the major countries of the world, irrespective of where creation of the work occurred.

Here are some of the requirements of the main types of work defined in law. You should note that this is a short summary of each area. The full Copyright

Act covers each of these areas in great detail and some areas of the Act require specialist legal interpretation.

Literary work — Literary works include not only novels, poetry and non-fiction books but also all other written works that are original. Length is important, as single words or short phrases may be denied copyright protection. It would be difficult to claim copyright for a short phrase of three words. However, in practice, letters, notes, directories, e-mail messages and World Wide Web (WWW) pages are usually protected. Computer programs and code are protected as literary works. Maps, charts and plans are not protected as literary works but as artistic works.

Dramatic work — Apart from plays, dramatic works in this context include instructions for dance or mime. To distinguish a dramatic work from a literary work, there must be some spoken words or described actions to perform.

Musical work — All types of musical scores including annotations and directions are covered in this section of the Act. The words of music are not regarded as musical works; they are protected as literary works.

Artistic work — Graphic works, photographs, sculptures and collages are protected regardless of artistic merit. However, works of architecture and of artistic craftsmanship are protected only if there is an artistic quality in the work.

Sound recording — This covers every type of sound recording on any type of medium from which sound can be reproduced.

Film — The definition of ‘film’ is any medium from which a moving image may be reproduced. The definition of film under the 1956 Act was similar, which thereby provided automatic protection for video recordings when video was developed. Thus moving images produced using animation are covered under this area of the Act.

Broadcasts — The definition of a ‘broadcast’ covers any transmission by wireless telegraphy that is capable of being lawfully received by members of the public. This includes satellite transmissions.

Cable programmes — These are transmissions carried as services by way of cable. This includes TV transmissions across the internet and also includes some online services such as certain online databases.

Published editions — There is copyright in the typography and layout of literary, dramatic and musical works. This is in addition to the protection given by musical work and literary work.

Performers' Rights

While not strictly speaking copyright, performers' rights provide protection to performers and persons who hold recording rights in a performance. Previously these were covered by legislation in the Performers Protection Acts of 1958, these rights are now included in the Copyright Protection Act.

Copyright Duration

The copyright given to protected works exists for a limited period only. This is called the 'term of copyright' and all works eventually emerge from copyright protection. There are some special instances where copyright can exist in perpetuity. Again as with the types of work, there are different lengths of copyright protection.

Moral Rights

Moral rights are different from copyright. Moral rights are not property rights; they give the creators of copyright works, including certain literary works, artistic works and films, three further rights:

1. The right for the author of a work to be acknowledged as the author or creator — the paternity right.
2. The right for anyone to object to his or her name being attributed to something he or she did not create.
3. The right not to have a work subjected to 'derogatory' treatment, that is, to some amendment that impugns the author's or creator's integrity or reputation.

The moral rights to a piece of work, unlike copyrights, are not transferable and therefore always remain with the creator, even if the creator has chosen to assign his or her copyright in the material.

With moral rights the creators also must choose to assert the first of the moral rights. Unlike the Copyright Act it is not an automatic right. You should also note that in some circumstances, moral rights can never exist, so for example if you are an employee who is paid to create copyright material in the course of your employment, you cannot acquire moral rights to that material.

Multimedia and Copyright

Traditionally, text is literary work copyright; still images are artistic work copyright; moving images are film or TV copyright; the spoken word is sound recording copyright; and musical works have their own copyright.

However, within multimedia, all of these items or some of the items are combined together into a single product. This may not present a problem if the arrangements for obtaining protection, the ownership, lifetimes and rules regarding these intellectual property rights were identical, but they are not.

The problem is compounded by the fact that the rules differ between countries, and yet multimedia, being in machine-readable form, can be passed from one country to another with trivial ease. It is this aspect that makes the use of the internet for the distribution of multimedia a copyright minefield.

There are four issues to consider:

1 Copyright laws vary from country to country. In some countries, for example, fair dealing is permitted for educational purposes, but not in others; the lifetime of copyright varies from country to country; the rules regarding who owns copyright in a film vary; the rights of performers of musical works vary, and so on.

2 Even within a country, the rules on the machine-readable text, still images, moving images, sound and music vary. In any multimedia work, there will be many copyrights, owned by different parties who often have different priorities and needs. The lifetimes of these copyrights vary significantly. Anyone wishing to copy or use a multimedia work can never be sure that (s)he has catered for all possible copyrights.

3 The various industries (publishing, computer software, films, broadcasting, photographic) are very different in terms of the sorts of licences they are prepared to agree. The traditions of the lifetime of licences, the royalties paid, and the safeguards for the copyright owner differ hugely depending upon the location.

4 It is often impossible to identify who owns the various rights in multimedia works. Copyrights are assigned and re-assigned, companies are formed and disappear, people move on and cannot be traced and yet, material cannot be copied without the copyright owner’s permission, and the law requires the potential user to go to considerable lengths to identify the owner and then gain permission if you are to reside within the law.

There is increasing pressure for governments to look at the questions of adopting a single uniform law for all multimedia, that is to make the regimes for text, sound, images, and so on, consistent, thereby at least simplifying the issues regarding ownership and lifetime.

The copyright implications of multimedia information delivery are enormous, and can only be touched upon. A multimedia publisher has to negotiate rights to all the components in the product with the many rights’ owners.

Internet and Copyright

E-mail messages, material loaded onto file transfer protocol (FTP) sites or WWW servers, and anything else put on the internet has some form of copyright attached. Of course if there is a statement waiving copyright then these issues do not arise. Just because materials are widely available and free of charge does not change the situation; there is not necessarily an implied license to copy. Therefore, you need to be careful about copying this type of material.

In practice unless the person who owns the materials makes a loss of income as a result of the copying there will generally not be a major problem.

Thus compilations of URLs or e-mail addresses are protected by copyright, as are internet indexes such as those created by Yahoo!, Alta Vista, and so on. The compilation of bookmarks within your browser, and your e-mail address book fall under the same category.

Downloading someone's WWW home page and using it as the basis of your own home page is clearly copyright infringement, and may also involve infringement of trademark rights if the WWW page includes a registered trademark. You need to create your own WWW page from scratch, amending someone else's copyright material is 'adaptation' in copyright law, and is infringement of the Act.

However, if you are a creator and you are worried about people ripping you off; the simple solution is do not put materials up on the internet. The problems of policing the internet, identifying infringements and then prosecuting offenders are enormous and, unless you are willing to spend very large sums of money, unworkable. If, on the other hand, you want to make it explicit that you waive all copyright to the material you are putting up on the internet, but still wish to retain your moral rights, you need to make a statement to this effect.

The Computer Misuse Act

With the widespread use of computer and communication systems, problems started to arise about the misuse of systems. The problems centred on a variety of uses that were not covered by existing laws. Several cases initially went to court but the courts were unable to convict because older laws did not cover these misuses. One particular case involved a schoolboy using his computer at home with a modem to hack into the Duke of Edinburgh's electronic mailbox and read his correspondence. Other schoolboy hackers were able to get through to stockbrokers, hospitals, oil companies and even the Atomic Energy Authority's computer systems. The courts were reluctant to use the theft laws as these were not intended to cover these situations, and they advised Parliament that it would need to make specific new laws to deal with this type of misuse. This gave rise to the Computer Misuse Act 1990.

Introduction

The Computer Misuse Act became law in August 1990. Under this Act hacking and the introduction of viruses became criminal offences. The following text summarises the types of offence. Full details about the Act can be found at the Office of Public Sector Information at http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Further summarised information about the act can be found at the Wikipedia site at http://en.wikipedia.org/wiki/Computer_Misuse_Act

Definition of Offences

The Act identifies three specific offences in relation to computer misuse:

1 Unauthorised access to computer material (that is, a program or data).

2 Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.

3 Unauthorised modification of computer material.

The Act defines (1) (the basic offence) as a summary offence punishable on conviction with a maximum prison sentence of six months or a maximum fine of £2000 or both. The Act goes on to describe offences (2) and (3) as criminal actions either summarily or on indictment, and punishable with imprisonment for a term not exceeding five years, a fine or both. These sentences for offences (2) and (3) clearly reflect the perceived gravity of the offence and would imply that everyone should take an equally serious view of hacking or virus proliferation.

All organisations including schools, colleges and universities are primarily concerned with preserving the integrity of shared computer systems and administrative systems.

In the event of any problem, systems managers would expect to take immediate remedial and preventive action and would expect the law to back them up in this action with penalties in place which would serve to discourage hacking, particularly the third category which could result in a valuable data being destroyed.

Definitions of Unauthorised Access

Example 1: Unauthorised Access to Computer Material

This would include: using another person's username and password without proper authority in order to use data or a program, or to alter, delete, copy or move a program or data, or simply to output a program or data (for example, to a screen or printer); laying a trap to obtain a password (keyboard logging programs); reading examination papers or examination results.

Example 2: Unauthorised Access to a Computer with Intent

This would include: gaining access to financial or administrative records, but intent would have to be proved. Intent in some circumstances will be difficult to prove if there is no material or financial gain to the access.

Example 3: Unauthorised Modification of Computer Material
This would include: destroying another user's files; modifying system files; creation of a virus; introduction of a local virus; introduction of a networked virus; changing examination results; and deliberately generating information to cause a system malfunction.

Preventive Measures — The simplest form of preventive action is publicity, and all opportunities should be used to make it clear that the institution will not tolerate this type of behaviour. The conditions of use for all computing facilities should spell out the seriousness of these activities.

Computer Security — The computer must be made secure with measures to combat hackers. There should be access control, user restrictions etc applied. The Computer Misuse Act has made the introduction of these types of measure assume even more importance.

Identifying the Offender — Finding and identifying someone who has hacked into or misused a system is a difficult and, above all, time-consuming task. It is sometimes possible to identify the person uniquely. More often it requires obtaining and presenting sufficient circumstantial evidence to persuade the individual to admit that the offence was committed.

Initiating Legal Procedures — All institutions need to be prepared to use the full powers of the Act for serious offences whether they originate within or without the organisation. It is normally the responsibility of the Police to initiate any action, but for a prosecution to be successful, evidence needs to be collected and kept as soon as misuse is suspected. In this type of case it is often prudent to seek technical and legal advice early in the proceedings.

Security and Integrity of Data

Data stored on computer is vital to the success of any business. The loss of computer files is an extremely serious problem for any organisation, so it is vital that businesses take steps to protect the security and integrity of data.

Security of data means keeping data safe from physical loss. This could be due to accidental damage, for example natural hazards such as flooding and fire, or it could be damage caused by hardware failure, for example when a tape gets caught up in a drive and is destroyed.

The loss of data could be intentional, for example theft by a competitor, unauthorised access (hacking), destruction by viruses or terrorism.

Integrity of data means the correctness of the stored data. Data may be incorrect because of errors in data transmission (caused by background noise on the line), input errors (data typed in wrongly), operator errors (for example an out-of-date version of the file has been loaded), program bugs, hardware breakdown, viruses or other computer crime.

Privacy of data means keeping data secret so that it cannot be accessed by unauthorised users. Since then, the Computer Misuse Act 1990 has made unauthorised access to computer material a criminal offence.

If a computer user orders goods by e-mail, they need to give their credit card number and expiry date. This is private information, which someone else might use to order goods fraudulently if the information was not kept secret.

Methods of Maintaining Security

There are many security procedures that organisations should use to maintain the security of their data and their computer systems.

The most obvious way is to lock the door to any computer installation. The lock can be operated by a conventional key, a 'swipe' card or a code number typed into a key-pad. Any code must be kept secret and should be changed frequently eg once per month.

Staff should not lend keys or swipe cards to anybody else. Locks activated by voice recognition, fingerprint comparison or eye retina scanning offer alternative but expensive, methods of security.

Additional security measures could include computer keyboard locks, closed circuit television cameras, security staff and alarm systems. Passive infra-red alarm systems to detect body heat and movement are commonly used, as they are reliable and inexpensive.

Computer systems with terminals at remote sites are a weak link in any system and must be fully protected. Disk and tape libraries also need to be protected; otherwise it would be possible for a thief to take file media to another computer with compatible hardware and software.

Staff and authorised visitors should wear identity cards, which should not be easily copied and should contain a photograph. These are effective and cheap security methods.

Of course all of these security methods are only effective if the supporting administrative procedures are properly adhered to, for example doors must not be left unlocked and security staff should check identity cards.

The security measures used by an organisation will reflect the value of the data stored and the consequences of data loss, alteration or theft. Financial institutions like banks and building societies need to have the very highest levels of security to prevent fraud.

Access to files must be controlled by passwords, which have to be keyed into the computer terminal in response to a series of questions displayed on the screen. There should be different levels of permitted access for different users depending on their needs.

Hackers are people who, acting illegally for fun or fraud, specialise in breaking through the software protection to gain access to a computer system or network system’s data and files. The passwords used within such systems need therefore to be carefully chosen, kept secure (memorised and not divulged) and changed very frequently.

The use of people's names, for example, is not a good idea as it may allow entry by guessing or by trial and error. Some computer systems only allow passwords which are not in a dictionary, as hackers may use programs that try every word in a dictionary until they get access.

The system should be aware of repeated unsuccessful attempts to gain access, as this is likely to be an unauthorised user. The network can be set up so that a computer is disabled after three wrong passwords have been entered and only able to restart after a certain time has elapsed. The network manager should be alerted by a message at the server if a number of wrong passwords have been entered in a short time.

A network access log can be kept. This keeps a record of the usernames of all users of the network, which station they have used, the time they logged on, the time they logged off, which programs they have used and which files they have created or accessed.

Security Procedures

It is important that users follow standard administrative procedures for maintaining security.

Passwords should be changed regularly and should never be left written down on scraps of paper. Whenever computer users leave their terminal, for example to see a colleague or to go to the toilet, they must log off so that unauthorised users cannot gain access. Other simple procedures may include:

- locking the keyboard to prevent unauthorised use
- using a virus check before using floppy disks from an unknown source
- not allowing unauthorised personnel to use your PC
- backing-up regularly.

Maintaining security is much harder if a company's computer system is connected to a public network like the internet. As many businesses today use the internet to make information available to other parts of the business or to suppliers, this presents a major security risk.

Firewalls can be used to protect the business's computers from intruders. A firewall is a single security point through which all traffic must pass. The firewall can use passwords to control traffic and can also log details of all access.

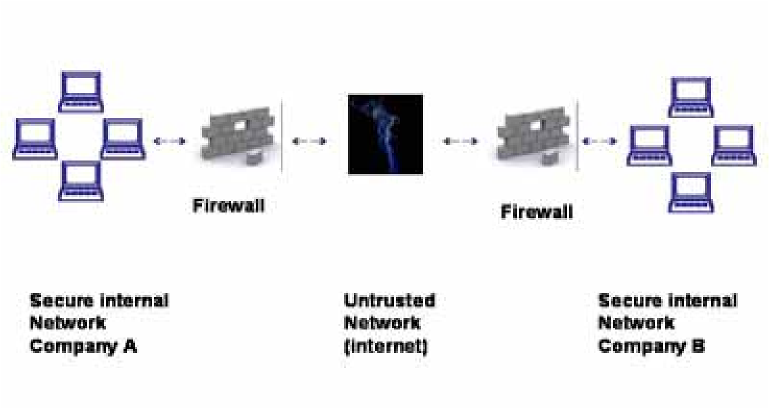
The Firewall

A *firewall* is an intelligent device or software program that is used to prevent unauthorised access to a network. The firewall is placed between the internal network and the external wide area network (internet). The firewall checks all communication between the internal and external networks and can be instructed to allow certain programs to access the internet whilst blocking others.

The firewall works in both directions so you can allow users to connect to and access your web server, but block all other access to the network. A firewall allows organisations to manage and control access easily, greatly reducing the risk of network break-in and the destruction or theft of data.

The Firewall Concept

A firewall is a system (hardware or software) that enforces a security policy between a secure internal network and an un-trusted network such as the internet. Firewalls tend to be seen as a protection between the internet and a private network. However, a firewall should be considered as a means to divide the world into two or more networks: one or more secure networks and one or more non-secure networks.



Photos © istockphoto.com – Pedro Tavares and Olga Zaichenko

The firewall can be a PC, a router, a Linux/Unix workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information and services from outside. Your firewall is usually installed at the point where the secure internal network and un-trusted external network meet.

In order to simplify the firewall concept, consider the network to be a building to which access must be controlled. The building has a lobby as the only entry point. In this lobby, receptionists welcome visitors, security guards watch visitors, video cameras record visitor actions, and badge readers authenticate visitors who enter the building.

Although these procedures can work well to control access to the building, what if an unauthorised person succeeds in entering, there is no way to protect the building against this intruder's actions. However, if the intruder's movements are monitored, it can be possible to detect any suspicious activity.

A firewall is designed to protect the information resources by controlling the access between the internal secure network and the un-trusted external network (the internet). However, it is important to note that even if the firewall is designed to permit the trusted data to pass through, deny the vulnerable services, and prevent the internal network from outside attacks, a newly created attack can penetrate the firewall at any time. In order to provide continual protection all logs and alarms generated by the firewall must be examined. Otherwise, it is not possible to protect the internal network from outside attacks.

Components of a Firewall System

As mentioned previously, a firewall can be a PC, a Unix/Linux workstation, a router, a combination of these or even software installed on specific computers or a router. Depending on the requirements, a firewall can consist of one or more of the following functional components:

Packet-filtering router

Most of the time, packet-filtering is accomplished by using a router that can forward packets according to filtering rules. When a packet arrives at the packet-filtering router, the router extracts certain information from the packet header and makes decisions according to the filter rules as to whether the packet will pass through or be discarded.

Application-level gateway (proxy)

An application-level gateway is often referred to as a *proxy*. An *application-level gateway* provides higher-level control on the traffic between two networks in that the contents of a particular service can be monitored and filtered according to the network security policy. Therefore, for any desired application, the corresponding proxy code must be installed on the gateway in order to manage that specific service passing through the gateway.

A proxy acts as a server to the client and as a client to the destination server. A virtual connection is established between the client and the destination server. Though the proxy seems to be transparent from the point of view of the client and the server, the proxy is capable of monitoring and filtering any specific type of data, such as commands, before sending it to the destination. For example, an FTP server is permitted to be accessed from outside. In order to protect the server from any possible attacks, the FTP proxy in the firewall can be configured to deny specific FTP commands.

For Further Information

For further detailed and specific firewall information check out the Wikipedia site which can be found at http://en.wikipedia.org/wiki/Firewall

Implementation of Security

Security procedures are only as good as the employees that use them. One of the most common breaches of a company's security is through its own employees. Industrial espionage does exist in the cut-throat competitive world of big business and it is not unknown for employees to be bribed to provide information to a rival.

Data may be altered or erased to sabotage the efforts of a company. Employees working in sensitive areas must be totally reliable and they will often be vetted before appointment. Strict codes of conduct exist for employees in this position and anyone found to have breached the organisation's regulations is likely to be instantly dismissed.

There are many ways in which the integrity of data can be affected. Many of the measures to ensure data security will also maintain data integrity. However data can be corrupted accidentally, for example through transmission errors, and businesses need to be aware of this. Again the methods of maintaining integrity will reflect the importance of accurate information.

Computer Crime

Computer crime is any criminal act that has been committed using a computer as the principal tool. As the role of computers in society has increased, opportunities for crime have been created that never existed before.

Computer crime can take the form of the theft of money (for example, the transfer of payments to the wrong accounts), the theft of information (for example, from files or databases), the theft of goods (by their diversion to the wrong destination) or malicious vandalism (for example, destruction of data or introducing viruses), the theft of identity (for example running up credit card debts, bank loans etc).

The rapid spread of personal computers and particularly, distributed processing, wide area networks and the internet, has made information held on computer systems more vulnerable.

Every one of the top 100 companies in the FTSE index has been targeted or actually burgled by this new type of computer criminal. The British police have evidence of 70,000 cases where systems have been penetrated and information has been extracted. One inquiry revealed three hackers had been involved in making 15,000 extractions from systems. These criminals are after information worth billions of pounds.

The arrival of automated teller machines (ATMs) provides a good example of how a new technological device creates new opportunities for fraudulent activity. In the 'phantom withdrawals' scandal, British banks and building societies were sued by hundreds of customers who claimed that they had been wrongly debited throughout the 1980s for withdrawals they did not make. The banks claimed that the customers must have withdrawn the money and that phantom withdrawals from their machines were 'impossible'.

In another case a criminal gang rented a shop, made it look like a bank and installed a fake cash-machine. The machine did not issue any money (saying it was out of order) but copied the magnetic strip on the back of each card and stored the card’s details and more importantly the card’s PIN number. The gang then made duplicate cards and used real cash machines to steal the actual money in the customers’ accounts. This was the first recorded instance of identity theft.

The widespread use of the mobile phone has led to another computer crime — cloning the chip inside the phone so that you can use your phone but the charge appears on someone else's bill.

Banking security experts in the USA estimate that an average bank robbery nets $1900 and the perpetrator gets prosecuted 82 per cent of the time. With a computer fraud, the proceeds are nearer to $250 000 and less than two per cent of offenders get prosecuted.

Software Copyright

The Computer Misuse Act 1990 which makes hacking illegal and The Data Protection Act 1984 which says how personal data on computer must be stored have been discussed. The widespread introduction of computers has led to new laws as well as new ways of breaking the old laws. Computer users must still also obey old laws such as The Copyright Act. So when you buy a software product you do not buy the program, you are only purchasing the right to use it. Thus, you do not have the right to give a copy to a friend.

If you own more than one computer, you should check the licence agreement which comes with your software to see if you have the right to run the software on more than one machine. Some licences are very strict — others are more open. Thus in some instances you may install the software on more than one machine but not have two people using the software at the same time. The most common licence agreements are:

- A *single-user licence* where the software can only be used on one machine. There are also small and home office licences (SOHO) which allow use across 3–5 machines.
- A *network licence* which may cover up to 15 or 20 stations on a network, depending on the licence. This type of licence is obviously much more expensive than a single-user licence.
- A *site licence* which enables the software to be used on any computer on the site. These are generally only applicable to large organisations.

The Federation Against Software Theft (FAST) aims to prevent illegal use of software and has a policy of prosecuting anyone found to be breaching copyright law. Software companies are getting more and more .sophisticated in their attempts to prevent breaches of copyright.

The program may only operate if a code is typed in. The code changes each time the program is run and can be found by contacting the supplier or manufacturer. Some programs will only run if the CD-ROM is in the CD drive or if a special piece of hardware called a dongle is plugged into the back of the computer.

The use of these types of protection has declined over the years, but some packages still use them.

Software Piracy

Software piracy involves the illegal copying of computer software. It is estimated to cost software developers around £9000 million per year. In 1998 it was estimated that about 86% of the software used in Europe and Asia was illegal. The figure has remained fairly constant over the years.

If a company has developed its own software rather than used off-the-shelf software it will have spent a lot of time and money on development. Large programs are usually written by a team, with each person writing a particular section or module. The number of person hours taken to write the programs can be large so the development costs need to be recovered by the sale of the software product.

Preventing Computer Crime

Good computer security is vital to protect information, but the Audit Commission has repeatedly reported that computer security is far too lax in most companies and government departments.

As more and more PCs become networked and connected to the internet, security problems will only get worse. Companies and individuals must not be complacent. Computer security undoubtedly is being improved quite rapidly, from fixing operating system errors, to firewall and anti-virus software but it seems that every time a security loophole is plugged, the computer criminals discover another one.

Detecting Computer Crime

When a fraud is found, some companies will not prosecute. For example, it would be too embarrassing for a bank to admit in court that its security was poor. There are plenty of stories about computer crime.

There is an old story of an American bank employee who rounded every interest calculation down to the nearest cent. All the leftovers from the calculation were sent to his own bank account. Over a period of years this it added up to millions but no one missed the odd half cent. In fact no one noticed that this was happening. Unfortunately, when he started to spend the money his jealous colleagues checked his bank account.

Computer crime is now such a big and specialist area that a new special police unit has been set up at New Scotland Yard to deal with it. Companies are vulnerable because they often underestimate the need for communication security.

They are at risk because they need their networks to keep in touch with personnel in the field and other offices.

Electronic Fraud

Electronic fraud is the use of computers or communication systems to commit fraud for financial gain. The main problem with this crime compared with traditional crimes is that the criminals tend to be quite intelligent and technically competent and therefore make considerable efforts to prevent discovery. They frequently see weaknesses in systems and set out to exploit them.

Electronic fraud often involves setting up false suppliers, who send invoices to a real company for payment. When payments are made to these fictitious suppliers the money is stolen. Great efforts are then taken to make sure that the real company's accounting system will still balance. Firms try to get around this type of fraud by making sure that several people are responsible for dealing with invoices so that to commit a fraud would need the co-operation of several members of staff.

Phantom Withdrawals

This is money which has been debited (taken out) mysteriously using an ATM without the person who owns the card, using it. This withdrawal of money usually only reveals itself when the customer checks their monthly statement. Although the courts have taken phantom withdrawals seriously, allowing groups of individuals jointly to take action for the return of their money, the banks have remained adamant that this cannot happen. In many cases, the banks say, the money has been removed by someone in the user's household who has borrowed a user's card and found the PIN number.

In order to combat this type of fraud many banks have a camera secretly concealed near the screen of the cash dispenser. This takes a picture of the person withdrawing the cash.

This picture is digitally compressed and stored on disk along with the details of the withdrawal, such as date, time, branch and account details.

Smart Cards

A *smart card* is a plastic card which contains its own built-in microchip, which performs two security functions. First it carries the holder's identification data and secondly it verifies this data against the PIN code that the cardholder enters at a card-reading terminal. In addition to this, the smart card can also hold details of the holder's credit limit and carry a record of the transactions made within this limit.

These are the basis for the chip and pin technologies that we use. However, the production of these types of card is relatively easy and it has been found that smart cards used to decode the TV signals transmitted by Sky have been successfully counterfeited. Bank cards are also just as easily counterfeited. Nevertheless, smart cards are used extensively in banking systems in many European countries.

Health and Safety

Thousands of computer users have blamed computers for various problems with their health over the years. Many trade unions representing these workers have claimed compensation from their employers and there is a legal basis for some claims.

It is widely accepted that prolonged work on a computer system can cause *repetitive strain injury* (*RSI*). This can be a serious and very painful condition that is far easier to prevent than to cure once contracted, and can occur even in young, fit individuals. It affects the shoulders, wrists and fingers of those typing on a keyboard all day at work. The symptoms are pain, numbness, stiffness, swelling and in severe cases paralysis.

RSI is often caused by a number of factors. Some of the main contributory factors have been identified as:

- overuse and repetition
- awkward or static posture
- insufficient recovery time
- a lack of RSI preventative products
- and of course, stress.

Most of these factors can be solved with some foresight by the organisation. Some of the recognised solutions to the problem are: the use ergonomic keyboards, the use of wrist supports and correct positioning of the chair being used by the individual. A statutory break time interspersed during the working day also helps to alleviate the occurrence of RSI type symptoms.

For Further Information

For further detailed information on the impact of RSI visit www.rsi-solutions.co.uk/

Working with Visual Display Units (VDUs)

Looking at a screen for a long time can lead to eye strain; particularly in glare or poor light, where screens flicker or where light from other sources is reflected in the screen.

A wide variety of work-related upper limb disorders may be associated with display use, as some users experience discomfort or aches and pains.

Where users experience difficulty, organisations should arrange for a reassessment of the work area to be carried out.

Eye effects: There are no known adverse effects on the eye or eyesight due to Display Screen Equipment (DSE) work. However, some users experience eye discomfort and may require advice on reducing this effect. It is very important that a person who does experience eye discomfort is able to adjust the DSE to ensure eye strain does not occur.

In order to reduce this type of eye strain the following possible solutions should be considered:

Non-flickering screens and screen filters to prevent glare and reflection are now required by law. However, with the widespread introduction of liquid crystal displays (LCD) the flickering that was common on the older display screens has been removed. Appropriate practices, for example, taking a break from the screen every few minutes should be encouraged. Appropriate spectacles should be worn when using a computer. Employers are now required to pay for employees’ eye-tests.

Common sense also plays a part and uncomfortable or awkward posture sitting at a computer can lead to serious back problems. Awkward foot positions may cause ankle problems. These are easily solved by providing an adjustable chair. This is a requirement under the law.

Also, employees have the right by law to be provided with foot supports which can reduce problems with ankles. Screens can tilt and turn to a suitable position.

Some general points would be:

- You should use a soft touch on the keys and not over-stretch your fingers.
- Your keyboard should adjust to get a good keying position.
- You may need a space in front of the keyboard to rest your hands and wrists while not keying.
- Your chair and monitor should adjust to find the most comfortable position for working.
- Your legs should be able to move freely under your desk.
- A footrest may be helpful.
- You should not sit in the same position for long periods. Try to change your posture occasionally.
- You should arrange your desk so that light is not reflected in the screen.
- You should have enough work space to take any documents you need.

Ozone

Laser printers emit ozone and so can become a health risk. Experts believe that ozone acts as an irritant, but it is harmless in the quantities present in printers. This has become more of a problem since the advent of affordable, small laser printers. Bubble jet or dot-matrix printers do not emit ozone.

Some possible solutions to reduce or remove this threat are:

- Personal laser printers should be located at least one metre away from where someone is sitting to avoid the ozone emissions.
- Ensure that there is good ventilation.

Other problems

Computers have also been blamed for the incidence of epilepsy in users.

The responsibility for the cause of health problems is very hard to prove, as they may have been the result of other activities. Eye strain may result from reading in poor light or watching too much TV, back and foot problems may result from wearing unsuitable shoes.

The following pages summarise some of the pertinent Acts that cover the Health and Safety issues that arise within an organisation that employs individuals. Some of the Acts cover schools, colleges and universities.

The Management of Health and Safety at Work Regulations

The regulations first took effect in 1993 and were revised in 1999. They placed certain duties and responsibilities on employers in relation to health and safety issues that arise in the work place.

A summary of the employer's duties include:

- To carry out assessments of risk to the health and safety of their employees, and to act upon risks they identify, so as to reduce them. (This is specified in Regulation 3.) This duty on employers, to carry out a risk assessment, is the area most highlighted by personal injury lawyers, to substantiate whether or not the employer has acted reasonably to provide a safe system of work.
- To appoint competent persons to oversee workplace health and safety.
- To provide employees with information and training on occupational health and safety.
- To operate a written health and safety policy.

For Further Information

Full details of the act can be found on the Office of Public Sector Information web pages at:

http://www.opsi.gov.uk/SI/si1999/19993242.htm

A summary of the Act can be found on the wikipedia pages at:
http://en.wikipedia.org/wiki/Health_and_Safety_at_Work_etc._Act_1974

The Workplace Health, Safety and Welfare Regulations

The main provisions of this 1992 Act require that employers must provide:

- Adequate lighting, heating, ventilation and workspace, to be kept in a clean condition.
- Staff facilities: toilets washing and refreshment.
- Safe passageways, eg preventing slipping and tripping hazards.

The Display Screen Equipment Regulations

The main provisions of this 1992 Act apply to display screen equipment (DSE). The users are defined as workers who use a computer as a significant part of their normal work. This includes people who are regular users of DSE equipment, or rely on it as part of their job. This Act comes into effect if you use DSE for an hour or more continuously, and/or you are making daily use of DSE.

Employers, by law are required to:

- Make a risk assessment of workstation use by DSE users, and reduce the risks identified.
- Ensure DSE users take adequate breaks.
- Provide regular eyesight tests.
- Provide health and safety information.
- Provide adjustable furniture (desk, chair, etc).
- Demonstrate that they have adequate procedures designed to reduce risks associated with DSE work, such as repetitive strain injury (RSI).

The Provision and Use of Work Equipment Regulations

The main provisions of this 1998 Act require employers to:

- Ensure the safety and suitability of work equipment for the purpose for which it is provided.
- Properly maintain the equipment, irrespective of how old it is.
- Provide information, instruction and training on the use of equipment.
- Protect employees from dangerous parts of machinery.

Disaster Recovery

It is important that computer users recognise the potential threats to their systems and the information they contain so that they can plan to avoid disasters leading to loss of data and have contingency plans to enable recovery of any lost data.

In an individual situation it may not be very serious if your computer system loses information and data. However, most of us now tend to use our computer system for storing more than our word processing work. We now use our computer systems to store music, photographs, movies etc. It is now becoming important for the private individual to consider the implications of data loss.

If disaster recovery plans and their management are inadequate then most commercial enterprises face serious data losses. In most instances they would be unable to process transactions which are at the heart of their business. Much of the day to day processing would cease. This would result in a loss of revenue and customers as they would be forced to go elsewhere. If this was to continue for any length of time, then there would be a loss of confidence in the organisation.

The statistics show that 75% of businesses without a recovery plan that suffer a serious data information loss never recover and go out of business.

How many times have you been in a supermarket when a power failure resulted in the organisation having to close their doors and cease trading as the cash registers (point of sales terminals) fail to function?

Potential Threats to Information

The threats to a computer information system are far ranging. Some of the major threats that need to be considered in any disaster recovery plan are covered below.

Physical Threats: Fire, Floods, Earthquakes or Terrorism

These physical disasters may be relatively rare, but when they do occur they can be devastating to your computer system. As well as the actual equipment, files containing vital data could be destroyed. Without disaster planning, many businesses would be unable to recover from the data loss. Many individuals would also suffer if there was data loss, but the effects would not be as severe. Many companies and organisations will employ specialist disaster recovery companies to manage their plans and oversee this important aspect of their business.

Hardware Failure

Hardware failure is a major cause of system breakdown and is quite common. Failure can arise from processor failure (generally rare) or disk head failure (quite a common occurrence). The failure of one hardware component can cause the whole computer system to crash. The growth in networks and distributed systems have in some ways made disaster recovery easier as it is possible for alternative sites to take over the functions of a site which has a hardware failure. On the other hand, as sites become more dependent upon each other, a failure at one location could easily cause universal shut-down across many sites.

Software Failure

Software can contain bugs which only occur when a particular combination of unusual events occur. Such bugs may not be detected in testing and lead to systems breakdowns at any time. They can be hard to locate and put right and cause considerable damage to data as well as delay in processing. Viruses can alter the way that programs function and lead to breakdown. Software can fail because it is unsuitable for the task or the volume of data may grow too big so that the software is not able to deal with it.

Problems Associated with Communication

The growth of data communications as wide area networks become wide spread poses data security problems as well as expanding the possibilities of breakdown. Data is very vulnerable to illegal access when travelling across the internal or external network. An organisation's IT security policy should state exactly how to prevent problems occurring and what to do if they do occur.

Risk analysis

Risk analysis involves determining what the risks are and designing appropriate counter measures. The risks will be different for different systems and will change over time.

The risk review may be made either on a quantitative basis. For example: expected annual loss = Probability of fire over 10 years (0.02) × cost of fire (£1,000,000); or on a subjective basis by consulting with staff and using knowledge of the business.

Any security incident can lead to loss of data confidentiality, integrity or availability which in turn may give rise to impacts of direct or consequential harm. The risk analysis provides a means of reducing risks to acceptable levels by implementing procedures to lessen the likelihood or impact of a threat.

All computer security involves reducing the risk to the electronic data. All risks are made up of three factors:

1 the potential threats to the data

2 its vulnerability and

3 its value to the organisation

Risk will increase if any of these factors increases. Thus *risk analysis* is the process of assessing vulnerability to threats, the potential losses, the current security controls and identifying possible counter measures to reduce risk.

It compares the cost of the potential loss with the cost of ensuring that the risk has a low probability of occurring.

Determining the threats against, and vulnerabilities of, a particular computer system is no easy task. The value of the data to the individual or the organisation will vary as each situation is unique, and the overall risk will differ.

Risks are assessed as:

Now — happening and tolerated (un-recoverable data errors)

Tomorrow — not happening but likely (hard disk failure, IDE drive failure)

Never (we hope) — unlikely but potentially catastrophic (fire, terrorist attack etc)

The criteria used in selecting appropriate measures are:

- the cost of implementing measures to protect against and recover from these types of failure
- the potential cost of the loss of data. Often underestimated.

The Disaster Recovery Plan

Any organisation or private individual that is in any way dependent on a computerised system, needs a plan which details how operations can be resumed after a disaster such as fire, flood, power disruption, or sabotage has disrupted its normal processing capability or destroyed its data.

In setting up a successful disaster recovery plan, it is essential to identify the most critical business functions and work out how each is vulnerable. It is then possible to establish the hardware, software, files, and human resources required to resume processing of these critical applications if any disaster occurs.

For successful recovery from the majority of disasters, data for critical applications must be backed-up and stored in a secure location. A business will have many backup tapes or disks, including the most recent global backup and several incremental backups.

Backup tapes must be date stamped as the order in which data is restored after any data loss is vital. The disaster recovery plan must include the order for restoring.

On an individual basis, the data may be stored in another location outside the general computer system area. But the general points stated above should be considered.

Contingency Plans

A *contingency plan* is a plan for recovery from a failure. It is a planned set of actions that can be carried out if things go wrong so that disruption is kept to a minimum. It is necessary first to identify what could go wrong and then what should be done if it did. For example, if you are organising an event to take place out of doors, it would be sensible to have a contingency plan in case of rain. Your plan could be to make a provisional booking in a local hall or provide guests with umbrellas!

As previously discussed there is much that can go wrong when using an IT based system, and it is important that any potential problems are identified before they occur. Some failures in a system can be avoided. Those that cannot be avoided, can, with an appropriate contingency plan in place, be prevented from having disastrous consequences.

The chances of damage from fire, tempest and flood can be minimised by having detectors in the computer room with CO_2 extinguishers available; by placing the computer room on the upper floor of the building and using fireproof safes for disks and backup tapes. Breakdown of power supplies can be avoided by having an uninterrupted power supply and a standby generator.

Malicious damage to the system can be addressed in part by having computer equipment in rooms protected by swipe card or other security methods. Strict codes of conduct need to be enforced to avoid illegal access to systems. For example, rules banning the use of personal floppy disks on the work stations can be established.

Hacking and associated problems could be countered by such measures as checking all accesses to the system, and only allowing three attempts before shutting down a terminal. The encryption of all data sent along communication channels internal and external should be considered.

Recovery of Data

Whatever precautions are taken, a disaster might still occur. It is only when such a disaster does occur that the adequacy of contingency plans can be seen. Loss of data should be avoided by keeping back-up copies on tape or on disk in case of problems.

General loss of data from a variety of causes can be addressed by backing-up the files on a regular basis and storing copies off site. Backing-up daily, that is overnight when the computer is less busy, is normally sufficient. More frequent backup may be needed in the case of constantly changing data and this can cause a problem.

Large organisations such as supermarkets and banks have more than one computer site in case of hardware problems. Contingency plans are set up so that the critical tasks of one site can be carried out at another.

Some simple measures to avoid disaster may be:

- Use of virus scanning software on all computer systems.
- Use of fault-tolerant components where redundant components switch in when trouble is identified.
- Use of smoke detectors in buildings.
- Uninterrupted power supply on key computer systems or standby generator.
- Strict password management and enforcement of password policies.
- Extra network links.
- Regular maintenance of all systems.

Implementing a backup and recovery strategy takes a lot of planning.

Security and Wide Area Networks (WANs)

Any data that is transferred on a network is vulnerable to misuse. This can be at a local level when the data is transferred between two machines on the same network or when the data is transferred across the internet.

Misuse can be intentional when an unauthorised user attempts to gain illegal access to a computer network. The risk of unauthorised access increases when data is transferred over a WAN using public communication links.

The people who attempt this type of illegal access are known as hackers. The latest figures suggest that if you connect an unprotected computer to the internet it will take on average 7 minutes before it has been hacked and under the control of hackers.

There are two main categories of hacker:

1 those who break into a system and
2 those who act as impostors.

It is a well known fact that there is no absolutely secure system, without eliminating all possibility of outside connection; a number of measures have to be taken to reduce the risk.

With a network system each account holder is issued with a unique identification number and chooses a secret password. Strict rules need to be applied to password choice, as described earlier in the text. Hackers can use software programs called *packet sniffers* to intercept identification numbers and passwords which travel across the network which are stored for later use. More secure systems can be designed to prevent the use of such programs.

The general method employed by most small businesses and private individuals to counter the effectiveness of ‘sniffer’ programs is the use of encryption. This is where the data is sent in a coded form that has to be decrypted on receipt before it can be understood.

The danger of break-in can be guarded against by the use of a firewall.

Network Security Issues

If the network belongs to a business organisation it will be maintained by the network administrator. The administrator’s duties will include installing software, allocating accounts and assigning initial passwords for users and making regular backups of data and software stored on the network.

Network Security

When an individual uses a stand-alone computer ensuring data is secure is a relatively simple matter.

- The use of a keyboard and disk lock can prevent other people from using the computer and accessing files.
- The use of a screen saver with a password can prevent casual prying when the user is away from their desk.

However, when the computer is part of a network, then security becomes a more complex issue. It is a requirement for network users to have an individual and unique username. This allows a directory space to be allocated to each user so that users are separated for each others' files. Generally you are assigned a password to connect to the computer network.

This provides security for a user. A user is usually only able to log on at one station at a time. The use of a unique username also allows the network manager to keep a record of who has been on the network and when and at which station they were working.

The user is allocated a username and an initial password. Once you have logged on for the first time you are requested to select your own password. This needs to be chosen with care, and obvious choices such as the user's name, pet's name, friend's name should be avoided. Ideally, the password should consist of a mixture of letters and numbers and should not spell out a meaningful word. Passwords should never be shared with others.

You may be connected to a system that requires a user to change their password on a regular basis, perhaps every month. Usually, the user is given a number (typically three) of grace logins, attempts at entering the correct password. If all attempts fail then the network manager is alerted and the user account is disabled for a period of time.

In a school or college environment, students will need to access shared software and files containing assignments created by their tutors /teachers. There needs to be a means of allowing different users different levels of access. Users can be assigned access rights to directories by the network administrator. These could be full rights (allowing the user to read, alter or delete files), or limited rights so that you can access a directory in read-only mode or access may be completely forbidden. In most instances users do not have access to each others' areas.

Access Rights

Some examples of access rights, which can be allocated to a user, are:

- administrator/supervisor
- read
- write
- create
- delete/erase
- modify
- file scan/list directory
- no access.

Viruses

A security hazard that is a serious problem with a network comes from viruses. Some viruses are simply annoying, making a program run unexpectedly whilst others can have catastrophic results.

On a stand-alone computer, the damage that can be done by a virus is fairly limited, whilst on a network it can destroy the files of a whole organisation. Viruses are transferred to systems from removable storage devices. These could be floppy disks, flash drives, USB sticks or MP3 players etc. In order to do this these devices have themselves been infected from another computer system.

Of course a threat will occur from public networks such as the internet. The main threat will be from downloaded files which may contain viruses. A number of measures should be put in place to help prevent a network becoming infected by a virus. You should always have virus checker running on the computer you are using. It is important to follow good practice to avoid infection.

Users can be forbidden from using a removable device in a networked computer without first checking it for viruses. By default most modern computers are set up to automatically check all files from such devices for virus infection.

Firewall software can be used with the internet to filter and check files that are down loaded. A firewall is a system placed between an internal network and the outside world which ensures that all traffic passing from the inside to the outside, or the outside to the inside, must pass through it. Only traffic which is authorised by the security policy is allowed to pass.

It is designed to protect a safe and trusted system from a risky and untrusted system.

Network Back-up

The need for backup becomes crucial when a network is in use as the implications of breakdown and data loss are larger than for a single computer system. Again good practice is important so for example, backing-up should occur regularly and backup copies should be checked as soon as they have been created to ensure that the process has been carried out correctly.

One of the most crucial requirements of maintaining security is the user. Computer users should be made aware, in a variety of ways, of the dangers of network use and the necessary precautions that should become an automatic part of their working habits.

Freedom of Information (Scotland) Act

The Freedom of Information Act 2002 is intended to act as a mechanism that will change the way public authorities approach openness and manage their records. The Act applies across the whole of the United Kingdom however; there is a slightly different Act which applies in England, Wales and Northern Ireland. Scotland has its own similar, though different, Act passed by the Scottish Executive on 28 May 2002.

The Act only applies to public authorities, including universities, schools, colleges and not private organisations. However, private organisations defined as a ‘publicly-owned company’ such as spin-off companies that are wholly or largely owned by a public authority are also subject to the Act.

There are two mechanisms for placing information in the public domain. Firstly, the Act establishes the right for any person making a request to a public authority to be informed in writing whether or not the authority holds the information. If it does hold the information then you should be supplied with that information subject to certain exemptions.

Secondly, it requires public authorities to make available information they hold and to publish a publication scheme which sets out the categories of information they intend to make readily available.

Right of Access

Under Part 1 of the Act, anyone may make a request for information to any public authority providing it is in writing, states the name and address of the enquirer and describes the information requested. You can make requests by e-mail or fax so long as they are legible and are capable of being used for subsequent reference.

The identity of the enquirer is of no concern to the authority and there are no restrictions as to nationality or residence.

The authority has a legal duty to confirm or deny whether or not it holds the information. If it does it must supply the information within 20 working days from receipt of the request. There are some exceptions.

Authorities are not obliged to provide information where they cannot find it without assistance and can make reasonable enquiries of the applicant in order to identify and locate the information requested. If such information is not received, the authority is not obliged to answer the request.

Where an applicant expresses a preference for the information to be supplied in a particular way, for example by asking for a hard copy of the information or a summary of it, the authority is obliged to do so wherever practicable or explain why it cannot. If no preferences are expressed by the applicant, the authority may supply the information by any reasonable means.

Exemptions

Part 2 of the Act sets out 23 exemptions where the right of access to information is either not allowed or is qualified. In the main, these relate to issues such as national security, law enforcement, commercial interests and data protection.

Information is also exempt under the Act if it is accessible to the applicant by other means such as a publication by another body. If this information is readily available under the authority's publication scheme, then it need not be provided in response to an individual request.

There are two general categories of exemption:

1. *Absolute Exemptions* — those where there is no duty to consider the public interest.
2. *Qualified Exemptions* — those where, even though an exemption exists, an authority has a duty to consider whether disclosure is required in the public interest.

The public interest test requires the authority to determine whether the public interest in withholding the information outweighs the public interest in disclosing it. This is performed by considering the circumstances of each particular case in the light of the potential exemption which might be claimed.

The balance in law lies in favour of disclosure since withholding must outweigh disclosure. In some cases, the duty to confirm or deny the holding of the information may still apply even if disclosure of the information itself would be against the public interest.

Fees

The authority may charge a fee for providing the requested information if it gives the applicant notice in writing to this effect before supplying the information. There is no obligation to supply the information until the fee is paid, and if the fee is not paid within three months, the request lapses.

The amount of fee charged has to take into account regulations guidance, including an upper limit. These are on a sliding scale and the authority is not obliged to provide more information than can be found for that cost.

For further information on the Act and the contents of the Act the following websites contain relevant information.

For Further Information

For a full text of the Act visit the following website: http://www.hmso.gov.uk/legislation/scotland/acts2002/20020013.htm.

There is a short summary of the act on the wikipedia site at: http://en.wikipedia.org/wiki/Freedom_of_Information_(Scotland)_Act_2002.

The Disability Discrimination Act

The Disability Discrimination Act (DDA) 1995 aims to end the discrimination that many disabled people face. This Act has been significantly extended by the Disability Discrimination Act 2005. It now gives disabled people rights in the areas of:

- employment
- education
- access to goods, facilities and services
- buying or renting land or property, including making it easier for disabled people to rent property and for tenants to make disability-related adaptations.

The Act now requires public bodies to promote equality of opportunity for disabled people. It also allows the government to set minimum standards so that disabled people can use public transport easily.

Further Information

The Department for Work and Pensions (DWP) website offers further information, including details on the changes made by the Disability Discrimination Act 2005. This site can be found at http://www.dwp.gov.uk/

The Wikipedia site at http://en.wikipedia.org/wiki/Disability_Discrimination_Act_1995 gives a detailed summary of the Act and the general implications of the act.

The Disability Rights Commission (DRC) website also has plenty of information, including a brief overview with the key points of the Act. It also provides full versions in PDF (both Acts) and word (DDA 2005 only) format. This site can be found at http://www.drc-gb.org/

A good summary of the topic =can be found on the Wikipedia site at http://en.wikipedia.org/wiki/Disability_rights_movement

How to Research

The process of research can be broken down into several components, for example: planning, searching, using the information, reporting the information, evaluating the information. It may be worth mentioning that not all of these are essential. Nevertheless, most academic research has all of these components.

Plan
Define your subject. You need to consider the topic or the question(s) you are trying to answer. What are you looking at, are there links to other areas? Try to produce a logical map of your approach. In order to do this you need to consider the following:

- What do you know? You should have some understanding of the problem. So put down what you know onto paper.
- Similar ideas. Are there areas, items that are similar? If so, jot them down — they might need to be looked at and they may be important aspects of your research under a different guise.
- Develop strategy. How are you going to get the work completed? You will have a timescale defined. This could be specified with the piece of work or it could be set by yourself. It is important that you set up a realistic time scale in which to produce your materials.
- Identify tools and resources. What exactly are you going to need to get the research completed? Remember that time is a resource, along with the magazines, books, journals, interviews etc.

Search for Information

- Library — Read widely and wisely. But you should remember that reading is not what research is about. Everyone has their own reading style. You can read the title, skim the abstract, look at the pictures and maybe the tables, and if there's anything interesting, then consult the text, looking for that specific point.

- Internet — Perhaps the resource that is over-used and overrated when performing research. The problem is that you suffer from information overload and can the materials be substantiated and validated? You need to carefully sift through the information and extract relevant pieces.
- Magazines/ Journals — These can be a good source of information but some specialist journals may have got into the habit of attending to a lot of details without explaining the overall specifics.

Take Notes and Use the Information

Which ever methods you use to obtain your information you need to compile it in note format for your own use. Some information that you initially gather may be worthless and not relevant, other information may be very relevant and open up new areas and ideas that you need to explore.

You may find yourself going into areas not previously contemplated and you always need to keep in mind that you have limited time resources. Learn to be ruthless and not to peruse all avenues of information.

Report

As soon as you have got information and a message to communicate, you should start writing your report. Do not wait until all your research is complete. It is better to write up your findings, revise and edit, revise and edit, revise and edit all the way through your piece of research.

The easiest parts to write are the results and what you did. You should write these first. What the results mean and drawing conclusions, recommendations etc. are altogether more problematic.

Evaluate

Evaluating any research is an essential part of the research process. There are a number of objectives that should be met during this process.

First and foremost the objectives that you set out at first should be met. You should identify successes and also perhaps failure. Any problems and weaknesses should be mentioned and solutions given to where these could be rectified.

Perhaps one key area is to provide information that might lead to further or future development. The evaluation process will help you to develop guidelines for the next piece of research that you become involved in.

For further information

The Wikipedia site at http://en.wikipedia.org/wiki/Research has a good outline description of the topic.

Finally

The student should (after consultation with their tutor) be able to do the Assessment for this Unit.

This completes all the learning outcomes for the PC Passport IT Security for Users subject. Students should ensure they carry our any relevant research required to further understand this subject.