Safety & Security in ICT Systems
INFO 2

Oliver Boorman-Humphrey

www.oliverboorman.biz

13 May 2013

This Time

This time we look at the need to protect data in ICT systems and the subsequent threats if these measures fail.

This section of the specification also looks at the physical protection of ICT systems and the legislation that covers the safety and security of data.

Threats to ICT systems

As ICT has developed, computer crime has increased. There are many threats to ICT systems and can be broken into two categories; Internal and External threats.

Examples of Internal threats include:

- ➔ Hardware failure
- ➔ Faulty procedures
- ➔ Poorly-trained staff
- ➔ Use of wireless networks
- ➔ Dishonest employees
- ➔ Disclosure of passwords

Examples of External threats include:

- ➔ Hackers
- ➔ Viruses & Malware
- ➔ Software, Music or Film pirates
- ➔ Denial of Service Attacks
- ➔ Fraudulent traders
- ➔ Paedophiles & Terrorists
- ➔ Organised criminals
- ➔ Money & Identity theft
- ➔ Natural disasters

Hacking

Any unauthorised access to computer data is illegal.

Unauthorised access to data held on an ICT system, from internal or external personnel, is called **hacking**.

Hacking often occurs in two forms:

- ➔ An employee or person who gains access to an ICT system to look at the data but not to change it;
- ➔ Gaining access to an ICT system to change the data in some way.

The motive for doing this ranges from employees boredom to espionage and stealing commercial material from another company.

Fraud

Fraud is the act of deliberate deception with the intention of gaining some benefit.

Internet fraud usually involves a criminal sets up a fraudulent site claiming to be a particular organisation, offering goods for sale. Unsuspecting customers buy the products which are never delivered although the money is transferred to the criminal. The criminal then has the credit card details allowing them to steal funds from the card.

This continues to be a problem as the Internet is not policed. The setting up of illegal financial websites or sending emails stating that they have come from a legitimate financial site is called **phishing**.

Piracy

As with money, the way we purchase music and software has changed.

It is now common place to download music, TV programmes, films and software from the Internet. This in most cases is legal, however people can visit illegal music sites and download the music illegally.

Even if you download a legal copy but then distribute it to others, it is considered piracy.

This costs the media industries millions of pounds every year in lost revenue.

Malpractice vs. Crime

Not all incidences of data lost from ICT systems are a result of illegal practices. There is the problem of **malpractice**.

For example, an employee who cannot remember their password and who decides to use a sticky note stuck to their computer screen acts in an unprofessional way. They are leaving their computer account open to hackers.

Another form of malpractice is to allow employees access to CD drives or USB pens so they can bring in software from home, this software will be unchecked and therefore may carry malware.

Malpractice is acting in an unprofessional way; it is not against the law but is against regulations set by the company.

Viruses

A program or file that can destroy or damage a computer system is called a **virus**.

Viruses often have the ability to replicate itself to try to increase the likelihood of causing damage.

Viruses can be spread while transferring data from computer to computer via portable storage devices, email, or while downloading files from the Internet.

Viruses

Limiting the risk of Viruses

Companies try to limit the risk of viruses and other malware being introduced into their IT systems. By:

- ➔ Preventing any unauthorised software being installed onto a machine;
- ➔ Preventing files being downloaded from the Internet;
- ➔ Ensuring portable storage devices from an outside source are not used;
- ➔ Ensuring emails from unknown email are not opened;
- ➔ Installing and running virus scanning software;
- ➔ Keeping the virus scanning software up to date.

Protecting Computer Systems

Most companies have strict procedures in place so that the sensitive data they hold is protected. These can include:

- ➔ Physical restrictions (swipe cards, servers in locked room etc);
- ➔ User names and passwords;
- ➔ User groups and access privileges;
- ➔ Audit trail software;
- ➔ Data scrambling using encryption;
- ➔ Data Backup;
- ➔ Careful vetting of staff;
- ➔ Training staff;
- ➔ Installing virus scanners;
- ➔ Installing a firewall;
- ➔ Uninterrupted power supply;
- ➔ Internet filters.

Levels of Access to Data

Users of a network are often supplied with a **username** and **password**.

The username *identifies* the user of the computer system whereas the password *authenticates* the user. Together they form the security of the system.

Different users have different access rights to the network; some are given simple access to an area but others, like the network manager, will have full access.

Levels of Access to Data

It is becoming more common to use biological features in place of username and passwords. **Biometrics** use previously recorded biological data to identify users.

This may include:

- ➔ Fingerprint Recognition
- ➔ Voice Recognition
- ➔ Face Recognition
- ➔ Iris Recognition
- ➔ Retina scans (compares pattern of blood vessels)

Legislation and regulations

Probably the most difficult part of the AS ICT course is learning about current Legislation that affects ICT use.

You do **not** have know lots of laws in depth, but you need to know about 5 important ones and what aspects they cover. Particularly,

- ➔ Computer Misuse Act 1990
- ➔ Copyright, Designs & Patents Act 1988
- ➔ Data Protection Act 1998
- ➔ Freedom of Information Act 2000
- ➔ Telecommunications Act 1996

Computer Misuse Act 1990

This act was introduced in order to cover a host of computer crimes that are not covered in pre-existing laws.

This law makes it illegal to:

- ➔ Deliberately plant a virus on a computer with the intention to cause damage;
- ➔ Use computers in work time to carry out unauthorised work;
- ➔ Copy computer programmes;
- ➔ Hack into someone elses system to view or change information;
- ➔ Use computers for fraud, e.g. fictitious employees on payroll.

The law came into effect before the roll-out of the Internet so it doesn't cover anything on the Internet.

Computer Misuse Act 1990

Categories:
Level I: Unauthorised access to computer material. Penalty: $£5000$ fine and/or 6 months in prison

Level II: Unauthorised access with intent to cause a further offence. Penalty: 5 years in prison

Level III: Unauthorised changing or deleting of files. Penalty: 5 years in prison plus fine.

Consequences:
When trying to decide whether an offence under this act has taken place, it is necessary to prove intent.

A court has to prove that the suspect intended to gain access to data and programs, didnt have the authorisation to do so, and *understood* that they didnt have authorisation.

Very few cases under the act have ever come to court.

Copyright, Designs and Patent Act 1988

The Copyright, Designs and Patents Act 1988 covers a wide range of data files such as music, literature and software.

This law makes it illegal to:

- ➔ Copy software;
- ➔ Install pirated software;
- ➔ Transmit software over a telecommunications line, thereby creating a copy;
- ➔ Use software without a proper licence.

Again, this law came into effect before the roll-out of the Internet but it does cover several activities on the Internet.

Copyright, Designs and Patent Act, 1988

Software Licensing: A software licence allows an individual to use a piece of software. Much of the cost when buying a piece of software is for the licence.

Typical types of Software Licence are:

- **Single User** - The user is allowed to install the software on a one or two machines. Only one copy can be in use at a time.
- **Multi-user** - Companies use this for software used on many computers. They specify the number of users that can use the software at any one time as opposed to the number of installs.
- **Network** - Allows the software to be run on a number of machines on a local network. Normally the maximum number of machines will be stated in the licence.
- **Site** - Allows the user to install the software on all machines they require - whether or not they are networked.

Data Protection Act 1998

This act of Parliament protects data (electronic and paper-based) and the privacy of the *subjects* which the data is about.

It has 8 main principles. Data must:

- be processed fairly and lawfully;
- be obtained only for a specific purpose and must not be processed in any other way;
- be adequate, relevant and not excessive for it's purpose;
- be accurate and where necessary up-to-date;
- not be kept longer than necessary for it's purpose;
- be processed in accordance with the rights of the data subject;
- be held securely;
- not be transferred to a country outside the EU unless there is adequate data protection legislation in operation.

Data Protection Act 1998

Some data is exempt from the Data Protection Act. Namely:

- Payroll, pensions, tax and accounts data;
- Household records;
- Statistical or research purposes, e.g. census;
- Crime and National Security data;
- News archives, literature and art;
- Mailing lists (as long as name and address only).

Data Protection Act 1998

The DPA protects **data subjects**. They are the living individuals who have personal data held about them on an ICT system.

The DPA allows individuals to have access to information held about them on a computer and where appropriate to have it corrected or deleted. It also gives the right to compensation for unauthorised disclosure of data.

A data subject does not need to give permission for data to be held about them; only if the data is sensitive does permission need to be sought. Sometimes consent is implicit, i.e. filling in a form, and anything pertaining to law, justice, and government does not need permission.

Data Protection Act 1998

Several people are involved in the DPA:

Data Controllers - Data controllers are those who control the contents and use of a set of personal data and liaise with the data subjects.

Information Commissioner - This is an independent official, appointed by the Crown, to oversee the Data Protection Act and the Freedom of Information Act and to report back to Parliament.

The Data Protection Registrar - Administers a Public Register of all Data Controllers. Also investigates complaints and initiates prosecutions for breaches of the act.

Freedom of Information Act 2000

This act sets the rules on access to information or records held by government bodies.

In general, such laws define a legal process by which government information is required to be available to the public.

In many countries, there are constitutional guarantees for the right of access to information. The UK has privacy and data protection laws in operation and these form a part of the Freedom of Information Act.

Telecommunications Act 1996

This act of parliament covers the duties of telecommunication carriers which include telephone and wireless companies.

It grants the licenses to broadcasting companies for television, satellite, cable and radio as well as for automated ship distress and air safety systems.

The act also regulates the scrambling of premium television services so that they are only accessible to those who pay. This part of the act can overlap onto the communication of premium material to and from a computer.

In 1997, an extra section was added to make it an offence to carry out fraud from online shopping. Prior to this, laws covering fraud did not include telecommunication links and therefore fraud was legal on the Internet!