Data Security and Privacy

Further reading:
1. GCSE C. Studies pg 283 – 285 2. Glossary Pg 111, 120-121 3. Merlin Pg 269 - 273

Data Privacy

Data privacy refers to the right of individuals or organizations to deny or restrict the collection and use of information about them. Data Privacy also requires system managers to reduce unauthorized access into their systems by building physical arrangements and software checks.

What is the data protection act?

The Data Protection Act is a law, which protects data on or about individual persons. According to this law, data must be;

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer then necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to countries without adequate protection

This act gives the *individual the right to know that data identifying them is being held, why it is being held and how it is being used.*

Data Security

Data security involves the use of various methods to make sure that data is correct, kept confidential and is safe.

Data security includes;

- Ensuring integrity of data.
- Ensuring privacy of data.
- Prevent the loss or destruction of the data

Loss or destruction of data can be prevented through two ways;

1. **Software Security** which consist of:

a) _____

Encryption software scrambles the data with a secret code so that no one can make sense of it while it's being transmitted. When the data reaches its destination, the same software unscrambles the information. When you see a small lock icon at the bottom of your browser, it indicates that your data will be encrypted during transmission.

b) _____

Most multiuser operating systems require a user to enter the correct user name and password before accessing the data, information, and programs stored on a computer or network.

Many other systems that maintain financial, personal, and other confidential information also require a user name and password as part of their logon procedure.

Some systems assign the user names and even passwords to their users, but some systems allow their users to choose their own user names and passwords.

c) _____

Many networks have audit controls to track which programs and servers were used, which files opened, and so on. This creates a record of how a transaction was handled from input through processing and output.

2. **Hardware Security** includes:
   - facilities to prevent accidental loss such as use of **write protect tabs** and making **backups**.
   - facilities to deter purposeful corruption of data such as **restricted access** to computer areas e.g. alarms
   - **Dongles** - Pieces of hardware which are used to reduce the possibility of software piracy. These usually plug into a standard interface on a computer. Without the correct dongle the protected software will not run

Unauthorised access and use of computers

Unauthorized access is the use of a computer or network without permission.
A **cracker**, or **hacker**, is someone who tries to access a computer or network illegally.
Some hackers break into a computer for the challenge. However, others use or steal computer resources or corrupt a computer's data.

Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities.
Examples of unauthorized use of computers include

- An employee using a company computer to send personal e-mail.
- Someone gaining access to a bank computer and performing an unauthorized transfer.

One way to prevent unauthorized access and unauthorized use of computers is to utilize an access controls which is a security measure that defines

- who can access a computer
- when the users can access the computer
- what actions the users can take while accessing the computer.

Access control is normally implemented using a two-phase process:

1. **Identification** verifies whether the user is a valid one.
2. **Authentication** verifies that the user is really the one he or she claims to be.

Different methods of identification and authentication exist. The most common is the use of User names and Passwords.

Data stored in computers is open to various **threats** such as stealing, hacking, natural disasters, virus infections, hardware damage, etc.

Software Piracy

According to estimates by the U.S. Software and Information Industry Association, as much as $7.5 billion of American software may be illegally copied and distributed annually worldwide. These copies work as well as the originals, and sell for significantly less money. Piracy is relatively easy, and only the largest rings of distributors are usually caught. Moreover, software pirates know that they are unlikely to serve hard jail time when prisons are overcrowded with people convicted of more serious crimes.

Software piracy refers to the unauthorized and illegal duplication of copyrighted software.

Software piracy is the most common form of **software theft**.

Purchasing a software only provides a consumer with a **license agreement**, or the right to use the software.

A single-user license agreement, is the most common type of license included with software packages which permit the consumer to install the software on only one computer system..

A software **site license** gives the buyer the right to install the software on multiple computers at a single site (e.g., a school computer laboratory).

A **network site license** allows network users to share a single copy of the software, which resides on the network server.

Risks of software piracy include

- Increase the chance of spreading computer viruses.
- No technical support for the software can be received.
- Increase the software cost for all legal users.

Software is protected in various ways against software theft (piracy);

- Hardware keys (dongles)
- Serial numbers
- Activation keys
- Software Registration

Backup

A **backup** is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed.

Files can be **restored** by copying the backed up files to their original location on the computer.

Backup copies should be kept in a fireproof and heatproof safe or **offsite**.

Some users implement a **three-generation backup** procedure to preserve three copies of important files.

- The **grandparent** is the oldest copy of the file.
- The **parent** is the second oldest copy of the file.
- The **child** is the most recent copy of the file.

Why backup?

- The disk drive you use for backups fails for mechanical reasons.
- Your computer is stolen - laptops are particularly vulnerable.
- Your computer is destroyed by fire, floods or other disasters.
- A power surge fries your machine.
- An employee accidentally or intentionally erases key data.
- A virus infects your system.
- Your hard drive crashes. Sooner or later it will; the only question is when.

What should be Backed Up?

The good news is that you don't need to make copies of all the files on your hard drive. These days, that could entail many gigabytes of data. You only have to back up your own data files, such as word processing documents, spreadsheets, e-mail, digital photos, graphics, etc. Basically, any files you've created or that were sent to you. You probably already have copies on CD-ROMs of your program files--Microsoft Office applications, web browsers, plug-ins and such. In the event that your computer crashes, you can use those to restore the programs or you can download replacement programs from the Net. So if we are using a desktop computer system we can use a CD-ROM to make a backup. But a mainframe computer system of a bank must use another type of storage media i.e. a tape for backup.