3-Security:

We all know why computers are taking over from human processors. They are much cheaper in terms of their cost/performance, can handle large volumes of transactions at great speed, do not make mistakes, are not members of workers' unions and do not take holidays or sick leave. In the early 1980's the computer was still an object of some mystery, hidden in large buildings and operated by specialist personnel. Today the computer is everywhere: in every office and many homes. However, computers also offer new chances for fraudulent and illegal activities.

Some of the issues that are addressed in this lecture include:

1. Security within the organization: fraud and access control.
2. Security beyond the organization: hackers and viruses.

1- Security Within the Organization:

Security risks within an organization include the processing of fraudulent transactions, unauthorized access to data and program files, and the physical theft or damage of equipment.

1.1- Fraud:

Computer fraud is increasing at a shocking rate. **Fraud** can be defined as the operation of the records of an organization to hide an illegal act (normally the theft of funds or other assets). The most common fraud tactics are:

- **Entering false transactions**. No special technical knowledge is required and the employee relies on the fact that management supervision of the process in weak.

- **Modification of computer files**. Normally requires a little more technical expertise as this would involve, for example, the increase or reduction of amounts held on the master file, which cannot be changed within the application (such as a payment).

- **Unauthorized changes to programs**. This type of fraud is usually limited to staff with programming expertise.

How does an organization limit fraud? There must be strong internal controls, separation of duties, restricted access to sensitive applications and constant management supervision.

1.2- Unauthorized Data Access:

Password protection is the most common method of protecting business data. One way to finding other user's passwords is through a **terminal spoof** - is a program that runs on a machine and looks like the normal login screen. Once a user has given his or her user-id and password, the terminal spoof will record both on the local disk or server, give error message (such as invalid password – please re-enter) and then passes control to the real login program. The criminal will pick up the passwords later to gain access to the system.

Other dangers of which managers should be aware include the **Trojan horse**, in which code is added to a program, which will activate under certain conditions.

Another risk is the **Back-door technique**. When programmers are building systems, they may try to avoid all the access security procedures to speed up the development time. In some cases, these "back doors" have not been removed and the programmer can gain illegal entry into the production system.

1.3 - Theft:

One famous case of theft involved a laptop computer stolen from the back seat of a car in the USA in early 1991. On the hard disk was the master plan for Desert Storm, the details of how the United States and her allies would attack Iraq.

Another form of theft relates to the copying of programs and data resources in an organization. Theft of software is a major problem in the PC world where users often make illegal copies of the programs rather than buying the package themselves – this practice is known as **software piracy.**

2- Security beyond the Organization:

2.1- Hackers and Firewalls:

Hackers are users from outside the organization, who enter a computer system usually through its communication lines. Although some hackers stealing the sensitive information (such as customers' credit card numbers).
A **firewall** is an additional system that applies access control policy between two networks, especially between a business network and the Internet. The firewall monitors all external communications, checks user authorization and maintains a log of all attempts to access the network. They can also be used to check for the existence of viruses, for the downloading of unauthorized software.
Encryption, which converts data into an unreadable form, can be used to improve data privacy and prevent any unauthorized changes to the message, as well as protecting the privacy of data within the organization.

2.2- Viruses

A computer **virus** is a program that attacks a computer system, normally by residing in corrupt files. The virus has the ability to replicate itself and so spread to other files and computer systems. Some viruses are gentle, but others corrupt the files they infect and even destroy entire databases.

There are three main types of viruses. ***Systems viruses*** resided in the boot sector of a disk. These viruses were usually easy to find and clean. One problem was that they loaded into memory as soon as an infected machine was switched on and could often hide them from the anti- virus software.

The next generation of viruses attached themselves to executable files. When an infected program is run, the virus resides in memory and infects all new programs run until the system is switched off. These viruses are difficult to counter, especially on a network as common files are often infected. Even when the file server is cleared of infected programs, users have copies on their personal hard drives or an infected copy of the program in memory when the virus check is performed on the server.
One area most users with which felt safe was the accessing of non-executable files such as word processing documents. Unfortunately there are now a number of ***macro viruses*** that can attach themselves to documents and spreadsheets. Even receiving a simple letter as an e-mail attachment can infect your machine.

Some of the more well known viruses include:

- ***Michelangelo***. This virus infected many machines in the early months of 1992. The virus was primed to activate on Michelango's birthday (6th March) and had the capability of destroying all files on the hard disk of infected PC's. News of the virus made headlines and many businessmen and home users rushed out to buying programs to check and clean viruses from their installations. On the day, some infections did occur but the main winners were the vendors of virus detection software.

- ***Stoned***. A very common virus in the late 1980's it came in many forms, some harmless while others corrupted files by attacking the directories and allocation tables. The main theme of the virus was normally the message "Your PC is now stoned" would appear on the screen.

- ***Concept***. A macro virus, attached to word processing documents.

- ***EXEBUG***. A nasty little bug that may corrupt your hard drive. This is a systems virus and can infect your PC. Very difficult to find and destroy as it uses "stealth" technology to hide from virus checkers.

The best line of defense against viruses is the regular use of up-to-date anti-virus software, which will scan files for viruses and remove them if found.