**COMPUTER SECURITY**

**What is Computer security?**

* Safeguarding the computer & the related equipment’s from the risk of damage or fraud

Protection of data & information against accidental or deliberate threats which might cause unauthorized modification, disclosure, or destruction.

A computer system can only be claimed to be secure if precautions are taken to safeguard it against damage or threats such as accidents, errors & omissions.

The security measures to be undertaken by the organization should be able to protect:

1. Computer hardware against damage.
2. Data, information & programs against accidental alteration or deletion.

* Data & information against hazards.

1. The computer against unauthorized use.
2. Data, information & programs against piracy or unauthorized copying.
3. Data & programs used by the computer system against illegal or unauthorized modification.

* Storage media, e.g., diskettes, tapes, etc. against accidental destruction.
* Policies of the organization.

1. Accidental interruption of power supply or communication lines.
2. Disclosure of confidential data or information.

* Ensure that both hardware & software have longer life span.

**Environmental threats to computers & Information systems.**

Fire destroys data, information, software & hardware.

***Security measures against fire:***

* Use fire-proof cabinets & lockable metal boxes for floppy disks.
* Use of backups.
* Install firefighting equipment’s, e.g., fire extinguishers.
* Have some detectors.
* Training of fire-fighting officers.
* Observe safety procedures, e.g., avoid smoking in the computer rooms.
* Have well placed exit signs.
* Contingency plans.
* **Water, floods & moisture.**

This causes rusting of the metallic components of the computer.

***Security measures against water, floods & moisture:***

* Set up computer rooms on higher grounds to avoid floods & humidity.
* Avoid installing computer components in the basement.
* There should be adequate drainage system.
* Use water-proof ceilings & floors.

**Lightening, electricity & electrical storms.**

This causes power failure that can cause damage to data, which has not been transferred to permanent storage devices.

***Security measures:***

* Install facilities to control power fluctuations, e.g., use of Uninterrupted power source (UPS)
* Use power stabilizers.
* Have standby power generators/sources.
* Have lightening arresters in the building.
* **Excessive Heat or Temperature.**

Excessive heat or temperature from the computer itself or from the surrounding environment can destroy computer storage media or devices.

***Security measures:***

* There should be efficient ventilation system.
* Use a cooling system in the computer rooms, e.g., cooling fans & air conditioners.
* **Computer virus attack.**

A **virus** is a rogue software program that spreads rampantly through computer systems, destroying data or causing the system to break down.

***Security measures against computer virus:***

* Make backup copies of software, and store the copies off-site.
* Restrict access to programs & data on a ‘need-to-use’ basis.
* Check all programs regularly for change of size, as this could be a sign of virus infiltration.
* Be careful with ‘Shareware’ and ‘Freeware’ programs, as they are the major entry points for viruses.
* Make sure all purchased software is in its original sealed-disk containers.
* **Smoke and Dust.**

Dust and Smoke particles settle on storage devices and may scratch them during Read/write operation.

***Security measures:***

* Have dust mats or carpets to prevent entry of dust.
* Fit the computer room with special Curtains to reduce entry of dust particles.
* Cover the devices with Dust covers when cleaning the room.
* Remove shoes before entering the room to prevent dust.
* **Terrorist attack.**

This includes activities such as:

* Political terrorists,
* Criminal type of activities,
* Individuals with grudges, or
* People intending to cause general destruction.

***Security measures:***

* Hiring of security guards to control physical access to the building housing the computer room.
* Activities that can cause terrorism should be avoided, e.g., exploitation of workers.
* Have double door & monitoring devices.
* Use of policies.
* System auditing / use of log files.
* Use of passwords.
* Punitive measures.
* Encryption of data.
* Use of firewalls.
* Consult & co-operate with the Police and Fire authorities on potential risks.

People threats include:

* Accidental deletion of data, information or programs.
* Vandalism, i.e., theft or destruction of data, information or programs & hardware.
* Piracy of copyrighted data & software.

***Security measures against Carelessness & Clumsiness:***

* Better selection of personnel.
* Have a good office layout.
* Improve employee training and education.
* Limit access to data and computers.
* Regular backups.
* Use of Undelete & Unformat utilities.

***Security measures against Vandalism:***

* Should have a sensitive attitude to office behavior.
* Tighten security measures, e.g., install alarm systems, burglar-proof doors/windows, & roofs).
* Limit access to sensitive company information.
* Use Keyboard lock on terminals used by authorized users.
* Use of disk locks.
* Punitive measures.

**CAUSES OF DATA LOSS IN COMPUTERS**

1. **Power failure:**

Momentary interruptions or fluctuations of electrical power may cause:

* Crashing of computers.
* Loss of data or information that had not been saved before the power disruption.
* Damage to computer’s secondary storage media. This may result to loss of data & Application software stored on the media.

The main cause of power disruptions are:

* Amplitude fluctuations,
* Power line *noise*,
* Low voltage *sages*,
* High voltage *surges*,
* Voltage *outages*,
* Voltage *spikes*,
* Waveform *distortions*,
* Power *frequency variations*.

**Precautions against data loss due to Power failure:**

1. *Regular saving of documents.*

Frequent saving of documents ensures that minimum data is lost in case of any power failure.

Some application packages have an**AutoSave** feature, which should be activated to automatically save work after a specified time interval.

1. *Use of Uninterruptible Power Supply (UPS).*

To eliminate any power quality defects or fluctuation, use power correction equipment such as a Stabilizer or Uninterruptible Power Supply (UPS).  These equipments ensure a steady flow of input power to the computer system.

1. **Computer viruses**

A computer virus destroys all the data files & programs in the computer memory by interfering with the normal processes of the operating system.

**Precautions against computer viruses:**

1. *Anti-virus software.*

Use Antivirus software to detect & remove known viruses from infected files.

Some of the commonly used Antivirus software are: Dr. Solomon’s Toolkit, Norton Antivirus, AVG Antivirus, PC-Cillin, etc

**NB**:  The best way to prevent virus is to have a memory-resident antivirus software, which will detect the virus before it can affect the system.  This can be achieved by installing a GUARD program in the RAM every time the computer boots up.  Once in the RAM, the antivirus software will automatically check diskettes inserted in the drives & warn the user immediately if a disk is found to have a virus.

* For an antivirus to be able to detect a virus, it must know its signature. Since virus writers keep writing new viruses with new signatures all the time, it is recommended that you update your antivirus product regularly so as to include the latest virus signatures in the industry.
* The Antivir
* us software installed in your computer should be enabled/activated at all times.
* You should also perform virus scans of your disks on a regular basis.
* Evaluate the security procedures to ensure that the risk of future virus attack is minimized.

1. **Accidental erasure:**

Commands such as DELETE & FORMAT can be dangerous to the computer if used wrongly.

Both commands wipe out the information stored on the specified secondary storage media, e.g., formatting the Hard disk (drive C:) will destroy all the software on that system.

**Precautions against Accidental erasure:**

1. *Use of Undelete utilities.*

Use the Undelete facilities in case you accidentally delete your files.

There are two Undelete facilities depending on the operating system you are using.

* **MS-DOS 6.0 Undelete facility**:

To undelete at the DOS prompt, change to the drive & directory whose files were deleted, then type, e.g.,

C:\>**UNDELETE <***directory that contain the deleted file***>**

A list of all deleted files will be displayed with the first letter missing.  Type in the first letter and the file will be recovered.

* **Norton utilities & PC Tools:**

Norton utilities & PC Tools also have an undelete facility, which is similar to the DOS Undelete facility.

* **Windows Recycle Bin:**

The Recycle Bin temporarily stores all deleted files & can be used to recover your files.

1. Double-click the Recycle Bin on the desktop.
2. Click on the files you want to undelete.
3. Click on **File**, choose **Restore**.

The Recycle Bin will restore all selected files to their original folders and disks.

**NB:**  If you delete a file accidentally, don’t copy any files or install any applications to the disk that contains the deleted file.  If you write anything to the disk, you might destroy parts of the deleted file, making it unrecoverable.

1. *Use of Unformat utilities.*

MS-DOS 6.0 has an Unformat facility which can be used to recover information stored on disks that have been accidentally formatted.

1. *Use of Backups.*

All data must be backed up periodically either on diskettes, tapes or CDs so that in case of any accidental loss, the backed up copy can be used to recover the data.

For small files, use the **Copy** command to make a copy of the data on a diskette.  For larger amounts of data, use the **Backup** command to copy the data to several diskettes or to a tape drive..

1. **Crashing of hard disks:**

When a hard disk crashes, the data or information on the disk cannot be accessed.  The effect is the same as formatting the hard disk.

Crashing of a hard disk can occur due to the following reasons:

1. Mishandling of the computer system, e.g.,

* Moving the system unit while the computer is on.
* Accumulation of dust.

1. Computer virus attack.

* Physical damage to the System unit caused by dropping or banging when being moved.

**Precautions against crashing of Hard disks:**

1. *Use of Backups.*

All data must be backed up regularly.  In addition, all application programs & operating system software should also be kept safely so that in case of a complete system crash, everything can be re-installed/restored.

1. *Use of Recovery tools.*

System tools such as Norton Utilities, PC Tools, QAPlus, etc can be used to revive a disk that has crashed.

* Steal large amounts of funds belonging to various companies by transferring them out of their computer accounts illegally.
* Steal or destroy data & information from companies, bringing their operations to a standstill.
* Spread destruction from one computer to another using virus programs. This can cripple the entire system of computer networks.
* Spread computer worm programs. Worm programs are less harmful in the beginning, but render the computer almost useless in the long-run.

**Precautions against Unauthorised access:**

1. *Restrict physical access.*

Physical access to computer systems should be restricted to ensure that no unauthorised person gets access to the system.

Some of the ways of restricting physical access include:

* Locking of doors.
* Use of personal identification cards.
* Use of fingerprint identification.
* Use of special voice-recorders. They analyse the voice of a trespasser & checks against the database containing the voice patterns of valid users.

1. *Password protection.*

Install a password to restrict access to the computer system.

A **Password** is a secret code that can be used to prevent unauthorised access of data in a computer.

Passwords can be put in at various levels:

* At the point of switching on the computer – to restrict access to the computer.
* On folders/directories – to restrict access to entire folders/directories.
* On files – to restrict access to individual files within a directory.
* On database systems – to restrict access to individual data elements.

When a valid password is entered, the user gets access to the computer system.  Usually, the user is allowed three (3) attempts to get the password correct.  If an invalid password is entered, access is denied after the 3 attempts.