DATA SECURITY AND CONTROL

Introduction

Data & Information must be protected against unauthorized access, disclosure, modification or damage. This is because; it is a scarce & valuable resource for any business organization or government. It is mostly used in transactions, it can be shared, and has high value attached to it.

Data & Information security:

Data security is the protection of data & information from accidental or intentional disclosure to unauthorized persons.

Data & Information privacy:

Private data or information is that which belongs to an individual & must not be accessed by or disclosed to any other person, without direct permission from the owner.

Confidential data or information – this is data or information held by a government or organization about people. This data/information may be seen by authorized persons without the knowledge of the owner. However, it should not be used for commercial gain or any other unofficial purpose without the owner being informed.

Review Questions

1. Differentiate between private and confidential data.
2. Why is information called a resource?
3. (a) Explain the term 'Information security'.
(b) Recently, data and information security has become very important. Explain.

SECURITY THREATS TO DATA & INFORMATION

1). *COMPUTER VIRUSES*

- A *computer virus* is a destructive program that attaches itself to other files when the files are opened for use, and installs itself on the computer, without the knowledge of the user.
- A *computer virus* is a program designed specifically to damage other programs or interfere with the proper functioning of the computer system.

A virus is a computer code usually designed to carry out 2 tasks:

(a) To copy itself from one computer system to another.
(b) To locate itself within a computer system enabling it to amend/destroy program & data files, by interfering with the normal processes of the operating system.

Types of computer viruses.

1. *Boot sector viruses* – they destroy the booting information on storage devices.

2. *File viruses* – they attach themselves to files either erasing or modifying them.

3. *Hoax viruses* – they come as e-mails with an attractive subject & activate themselves when the e-mail is opened.

4. *Trojans* – they appear to perform necessary functions, but perform other undesirable activities in the background without the knowledge of the user.

5. *Worms* – viruses that stick in the computer memory.

6. *Backdoors* – may be a Trojan or Worm that allows hidden access to a computer system.

Types of destructions/damages caused by a virus attack.

- Delete or modify data, information & files on storage devices (disks) or memory during normal program execution, e.g., may attack the format of a disk making any program or data on it impossible to recover.
- Systematically destroy all the data in the computer memory.
- Might lock the keyboard.
- Can change keystroke values or data from other I/O devices, e.g., change the effect of SHIFT key.
- Delete characters displayed on a visual display.
- Uses up computer memory/space, hence slowing down its performance or causing the system to crash.
- Changes colour of the display.
- Cause boot failure.

Sources of viruses.

a) ***Contact with contaminated systems:***

If a diskette is used on a virus infected computer, it could become contaminated. If the same diskette is used on another computer, then the virus will spread.

b) ***Use of pirated software:***

Pirated software may be contaminated by a virus code or it may have been amended to perform some destructive functions which may affect your computer.

c) ***Infected proprietary software:***

A virus could be introduced when the software is being developed in laboratories, and then copied onto diskettes containing the finished software product.

d) ***Fake games:***

Some virus programs behave like games software. Since many people like playing games on computers, the virus can spread very fast.

e) ***Freeware and Shareware:***

Both freeware & shareware programs are commonly available in Bulletin board systems.
Such programs should first be used in controlled environment until it is clear that the program does not contain either a virus or a destructive code.

f) ***Updates of software distributed via networks:***

Viruses programs can be spread through software distributed via networks.

Symptoms of viruses in a computer system.

The following symptoms indicate the presence of a virus in your computer:

- Boot failure.
- Files & programs disappearing mysteriously.
- Unfamiliar graphics or messages appearing on the screen, e.g., the virus might flash a harmless message such as "*Merry Christmas*" on the computer terminal.
- Slow booting.
- Gradual filing of the free space on the hard disk.
- Corruption of files and programs.
- Programs taking longer than usual to load.
- Disk access time seeming too long for simple tasks.
- Unusual error messages occurring more frequently.
- Frequent read/write errors.

- Disk access lights turning on for non-referenced devices.
- Computer hags anytime when running a program.
- Less memory available than usual, e.g., Base memory may read less than 640KB.
- Size of executable files changing for no obvious reason.

Control measures against viruses.

i). Install up-to-date (or the latest) antivirus software on the computers.

ii). Restrict the movement of foreign storage media, e.g., diskettes in the computer room. If they have to be used, they must be scanned for viruses.

iii). Avoid opening mail attachments before scanning them for viruses.

iv). Write-protect disks after using them.

v). Disable floppy disk drives, if there is no need to use disks in the course of normal operation.

vi). Backup all software & data files at regular intervals.

vii). Do not boot your computer from disks which you are not sure are free from viruses.

viii). Avoid pirated software. If possible, use the software from the major software houses.

ix). Programs downloaded from Bulletin Boards & those obtained from computer clubs should be carefully evaluated & examined for any destructive code.

2). *UNAUTHORIZED ACCESS*

Data & information is always under constant threat from people who may want to access it without permission. Such persons will usually have a bad intention, either to commit fraud, steal the information & destroy or corrupt the data.

Unauthorized access may take the following forms:

a). ***Eavesdropping:***

This is tapping into communication channels to get information, e.g., *Hackers* mainly use eavesdropping to obtain credit card numbers.

b). ***Surveillance (monitoring):***

This is where a person may monitor all computer activities done by another person or people.
The information gathered may be used for different purposes, e.g., for spreading propaganda or sabotage.

c). ***Industrial espionage:***

Industrial espionage involves spying on a competitor so as to get or steal information that can be used to finish the competitor or for commercial gain.
The main aim of espionage is to get ideas on how to counter by developing similar approach or sabotage.

d). An employee who is not supposed to see some sensitive data gets it, either by mistake or design.

e). Strangers who may stray into the computer room when nobody is using the computers.

f). Forced entry into the computer room through weak access points.

g). Network access in case the computers are networked & connected to the external world.

Control measures against unauthorized access.

i). Enforce data & information access control policies on all employees to control access to data.

ii). Keep the computer room closed when nobody is using it.

iii). Reinforce weak access points, e.g., doors & windows with metallic grills & burglar alarms.
iv). Use file passwords to prevent any person from getting access to the electronic files.
v). Enforce network security measures, e.g., use of firewalls.
vi). Encrypt the data & information during transmission.
vii). Perform frequent Audit trails to identify threats to data & information.

3). *COMPUTER ERRORS & ACCIDENTAL ACCESS*

Errors and accidental access to data & information may be as a result of:

- Mistakes made by people, e.g., one may print sensitive reports & unsuspectingly give them to unauthorized persons.
- People experimenting with features they are not familiar with. E.g., a person may innocently download a file without knowing that it is self-installing or it may be dangerous to the system.

Control measures against computer errors & accidents.

i). Restrict file access to the end-users and technical staff in the organization, i.e., deny access of certain files & computers to certain groups of end-users.

This is because; accidental access mistakes occur if the end-users have too much privilege that allows them to access or change sensitive files on the computer.

ii). Set up a comprehensive error-recovery strategy in the organization.

4). *THEFT*

The threat of theft of data & information, hardware & software is real. Some information is so valuable such that business competitors or some governments can decide to pay somebody a fortune so as to steal the information for them to use.

Control measures against theft of information, hardware, & software.

i). Create backups & store them in locations away from the main computing centre.
ii). Reinforce weak access points, e.g., the windows, doors, & roofing with metallic grills and strong padlocks.
iii). Put burglar proofs in the computer room.
iv). Employ guards to keep watch over data & information centres and backups.

Review Questions

1. Explain any three threats to data and information.
2. Give two control measures one would take to avoid unauthorized access to data and information.
3. Explain the meaning of ‘industrial espionage’.
4. (a) Define a computer virus.
(b) Give and explain two types of computer viruses.
(c) List three types of risks that computer viruses pose.
(d) List and explain five sources of computer viruses.
(e) Outline four symptoms of computer viruses.
(f) Explain the measures one would take to protect computers from virus attacks
5. How can one control the threat of user’s errors to data and information?

COMPUTER CRIMES

- A **computer crime** is a deliberate theft or criminal destruction of computerized data.
- The use of computer hardware, software, or data for illegal activities, e.g., stealing, forgery, defrauding, etc.
- Committing of illegal acts using a computer or against a computer system.

Types of computer crimes.

The following are the major types of computer crimes:

1. Trespass.
2. Hacking.
3. Tapping.
4. Cracking.
5. Piracy.
6. Fraud (Theft of money)
7. Sabotage.
8. Alteration of data.
9. Theft of computer time / Theft of service.
10. Theft of data, information or programs.
11. Damage of software.

Trespass.

- **Trespass** refers to the illegal physical entry to restricted places where computer hardware, software & backed up data is kept.
- It can also refer to the act of accessing information illegally on a local or remote computer over a network.

Trespass is not allowed and should be discouraged.

Hacking.

Hacking is an attempt to invade the privacy of a system, either by tapping messages being transmitted along a public telephone line, or through breaking security codes & passwords to gain unauthorized entry to the system data and information files in a computer.

Reasons for hacking.

- To copy or corrupt the information.
- As a hobby to test their expertise. Some people like the challenge & they feel great after successful hacking.
- Some do it for computer & software producing companies that want to secure their systems by reducing weaknesses discovered after professional hacking.

Hacking is done by skilled programmers referred to as **Hackers**. **Hacker** is a person who gains unauthorised access to a computer network for profit, criminal mischief, or personal gain.

Such people are able to break through passwords or find weak access points in software. They are involved in propagating computer viruses.

Tapping.

Tapping involves listening to a transmission line to gain a copy of the message being transmitted.

Tapping may take place through the following ways:

a) A person may send an intelligent program to a host computer that sends him/her information from the computer.

b) Spying on a networked computer using special programs that are able to intercept messages being sent & received by the unsuspecting computer.

Cracking.

Cracking is the use of guesswork by a person trying to look for a weakness in the security codes of a software in order to get access to data & information.

These weak access points can only be sealed using sealed using special corrective programs called *Patches*, which are prepared by the manufacturing company.
A **program patch** is a software update that when incorporated in the current software makes it better.

NB: Cracking is usually done by people who have some idea of passwords or user names of the authorized staff.

Piracy.

Software, information & data are protected by copyright laws. **Piracy** means making illegal copies of copyrighted software, data, or information either for personal use or for re-sale.

Ways of reducing piracy:

i) Enact & enforce copyright laws that protect the owners of data & information against piracy.
ii) Make software cheap enough to increase affordability.
iii) Use licenses and certificates of authenticity to identify originals.
iv) Set installation passwords that prevent illegal installation of software.

Fraud.

Fraud is the use of computers to conceal information or cheat other people with the intention of gaining money or information.

Fraud may take the following forms:

a). *Input manipulation:*

Data input clerks can manipulate input transactions, e.g., they can create dummy (ghost) employees on the Salary file or a ghost supplier on the Purchases file.

b). *Production & use of fake documents:*

E.g., a person created an intelligent program in the Tax department that could credit his account with cents from all the tax payers. He ended up becoming very rich before he was discovered.

Fraudsters can either be employees in the company or outsiders who are smart enough to defraud unsuspecting people.

Reasons that may lead to computer fraud.

- For economic gain (i.e., to gain money or information).
- To gain respect (self-worth)

Security measures to prevent fraud:

i) Careful recruitment of staff.
ii) Set up a clear & firm management policy on crimes & frauds.
iii) Restrict access to computer room or terminal.
iv) Use transaction & fill logs to monitor access to sensitive areas of the system.
v) Monitor & investigate error logs and reports on regular basis.
vi) Carry out risk analysis to examine the exposure of the organization to possible fraud.

Sabotage

Sabotage is the illegal or malicious destruction of the system, data or information by employees or other people with grudges with the aim of crippling service delivery or causing great loss to an organization.

Sabotage is usually carried out by discontented employees or those sent by competitors to cause harm to the organization.

The following are some acts of saboteurs which can result in great damage to the computer centres:

- Using Magnets to mix up (mess up) codes on tapes.
- Planting of bombs.
- Cutting of communication lines.

Alteration.

Alteration is the illegal changing of stored data & information without permission with the aim of gaining or misinforming the authorized users.

Alteration is usually done by those people who wish to hide the truth. It makes the data irrelevant and unreliable.

Alteration may take place through the following ways:

a). *Program alteration:*

This is done by people with excellent programming skills. They do this out of malice or they may liaise with others for selfish gains.

b). *Alteration of data in a database:*

This is normally done by authorized database users, e.g., one can adjust prices on Invoices, increase prices on selling products, etc, and then pocket the surplus amounts.

Security measures to prevent alteration:

i) Do not give data editing capabilities to anybody without vetting.

ii) The person altering the data may be forced to sign in order for the system to accept altering the information.

Theft of computer time.

Employees may use the computers of an organization to do their own work, e.g., they may produce publications for selling using the computers of the company.

Theft of data (i.e., commercial espionage).

Employees steal sensitive information or copy packages and sell them to outsiders or competitors for profit.
This may lead to a leakage of important information, e.g., information on marketing strategies used by the organization, research information, or medical reports.

Review Questions

1. (a) Define the term ‘Computer crime’.
(b) State and explain various types of computer crimes.
2. Differentiate between Hacking and Cracking with reference to computer crimes.
3. What is a program patch? Why are patches important?
4. Give two reasons that may lead to computer fraud.
5. How can piracy be prevented in regard to data and information.
6. What is data alteration? Explain its effects on data.
7. Explain the meaning of Tapping while dealing with computer crimes.

DETECTION & PROTECTION AGAINST COMPUTER CRIMES

The following measures can be taken to detect & prevent computer crimes, and also seal security loopholes.

Audit trails

This is a careful study of an information system by experts in order to establish (or, find out) all the weaknesses in the system that could lead to security threats or act as weak access points for criminals.

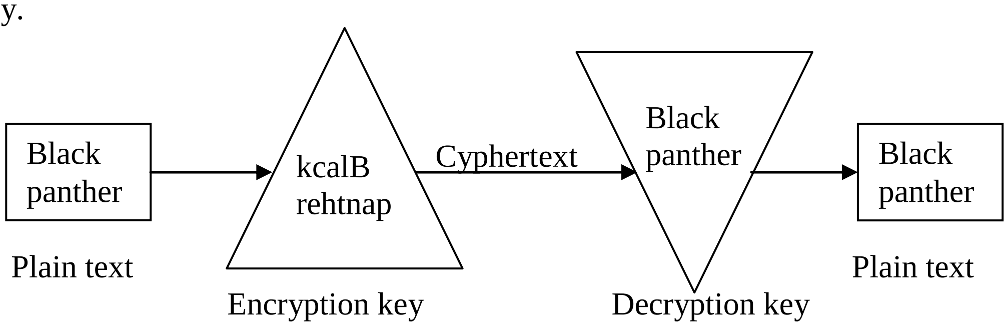
An audit of the information system may seek to answer the following questions: -

1. Is the information system meeting all the design objectives as originally intended?
2. Have all the security measures been put in place to reduce the risk of computer crimes?
3. Are the computers secured in physically restricted areas?
4. Is there backup for data & information of the system that can ensure continuity of services even when something serious happens to the current system?
5. What real risks face the system at present or in future?

Data encryption

Data being transmitted over a network faces the dangers of being tapped, listened to, or copied to unauthorized destinations.
To protect such data, it is mixed up into a form that only the sender & the receiver can be able to understand by reconstructing the original message from the mix. This is called **Data encryption**.

The flow diagram below shows how a message can be encrypted and decrypted to enhance security.



The message to be encrypted is called the *Plain text* document. After encryption using a particular order (or, algorithm) called *encryption key,* it is sent as *Cyphertext* on the network.
After the recipient receives the message, he/she decrypts it using a reverse algorithm to the one used during encryption called *decryption key* to get the original plain text document.
This means that, without the decryption key, it is not possible to reconstruct the original message.

Log files

These are special system files that keep a record (log) of events on the use of the computers and resources of the information system.

Each user is usually assigned a *username* & *password* or account. The information system administrator can therefore easily track who accessed the system, when and what they did on the system. This information can help monitor & track people who are likely to violate system security policies.

Firewalls

A **Firewall** is a device or software system that filters the data & information exchanged between different networks by enforcing the access control policy of the host network.

A firewall monitors & controls access to or from protected networks. People (remote users) who do not have permission cannot access the network, and those within cannot access sites outside the network restricted by firewalls.

LAWS GOVERNING PROTECTION OF INFORMATION

Laws have been developed that govern the handling of data & information in order to ensure that there is 'right of privacy' for all people.

The following rules must be observed in order to keep within the law when working with data and information.

1. Data & information should be kept secure against loss or exposure.
2. Data & information should not be kept longer than necessary.
3. Data & information should be accurate and up-to-date.
4. Data & information should be collected, used & kept for specified lawful purposes (i.e., it should not be used for unlawful gain).
5. The owner of the data has a right to know what data is held by the person or organization having it.
6. Data should not be transferred to other countries without the owner's permission.
7. Do not collect irrelevant and overly too much information for a purpose.

Review Questions

1. What do the following control measures against computer crimes involve?
(i) Audit trail.
(ii) Data encryption.
(iii) Log files.
(iv) Firewalls.
2. Give four rules that must be observed to keep within the law when working with data and information.

COMPUTER SECURITY

What is Computer security?

- Safeguarding the computer & the related equipments from the risk of damage or fraud.
- Protection of data & information against accidental or deliberate threats which might cause unauthorised 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:

i) Computer hardware against damage.
ii) Data, information & programs against accidental alteration or deletion.
iii) Data & information against hazards.
iv) The computer against unauthorised use.
v) Data, information & programs against piracy or unauthorised copying.
vi) Data & programs used by the computer system against illegal or unauthorised modification.
vii) Storage media, e.g., diskettes, tapes, etc against accidental destruction.
viii) Policies of the organization.
ix) Buildings.
x) Accidental interruption of power supply or communication lines.
xi) Disclosure of confidential data or information.
xii) Ensure that both hardware & software have longer life span.

Environmental threats to computers & Information systems.

1). <u>Fire.</u>

Fire destroys data, information, software & hardware.

Security measures against fire:

– Use fire-proof cabinets & lockable metal boxes for floppy disks.
– Use of backups.
– Install fire fighting equipments, 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.

2). <u>Water, floods & moisture.</u>

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.

3). <u>Lightening, electricity & electrical storms.</u>

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.

4). 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.

5). 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.

6). 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.

7). 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.

8). <u>People.</u>

People threats include:

- Carelessness.
- Clumsiness.
- 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 behaviour.
– 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 authorised users.
– Use of disk locks.
– Punitive measures.

9). <u>Earthquakes.</u>

Review Questions

1. (a) What is Computer security?
(b) Mention various threats to computer security.

2. Discuss the environmental problems affecting the operation of computers.

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:

a) *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.

b) *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.

2. 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:

a) *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 Antivirus 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.

Review Questions

1. Describe two ways of preventing data loss due to power outage.

2. (a) What is a Computer virus?
(b) What are Anti-viruses? Explain how they detect and remove viruses.

3. 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:

a) *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.

b) *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.

c) *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.

Review Questions

1. Name two commands that can erase the information from a disk.
2. Define 'Data backup' and state its importance.

4. 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:

i) Mishandling of the computer system, e.g.,
– Moving the system unit while the computer is on.
– Accumulation of dust.
ii) Computer virus attack.
iii) Physical damage to the System unit caused by dropping or banging when being moved.

Precautions against crashing of Hard disks:

a) *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.

b) *Use of Recovery tools.*

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

Review Questions

1. List two possible causes of a hard disk crash.

5. Unauthorised access:

Unauthorised access refers to access to data & information without permission.

Computer criminals can do the following harms:

- 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:

a) *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.

b) *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.

Some computer security systems may generate an alarm if someone tries to use a fake password.

NB: You should never use passwords that can easily be linked to you, e.g., your name, birth date, or names of people close to you.

Review Questions

1. State and discuss four causes of data loss in a computer system.

2. (a) Discuss two methods used to restrict unauthorised access to computer systems.

(b) What is a Password? Give its main importance.