

Unit 6 Data Security and Controls

Introduction and Definition of terms

Introduction There has been a rapid use of technology worldwide. This has led to rise of vices such as cybercrime, terrorism and cyber bullying. These vices have prompted the need to protect data and improve privacy over the internet.

Definition of terms

Data security: It refers to measures that are applied to prevent unauthorised access, loss and modification of data in computer systems and databases.

Data privacy: It is the ability of an organisation to control what data in a computer system can be shared to the third party.

Confidential data: Refers to data belonging to an individual that is held by an organisation for official use only.

Data integrity: Refers to the timeliness, correctness and confidentiality of data.

Differences between data privacy and data security and operational methods to ensure the safety of the data

Data privacy	Data security
Data is accessed by, or disclosed to authorised persons only.	Makes sure that data is correct, available, safe and is kept confidential.
Deals with appropriate use of data.	Deals with collecting only the required data , its safety and destroying data that is not needed.

Operational methods to ensure the safety of data

- Use of passwords to access data.
- Use of access levels.
- Using screen-savers to hide the contents of the screen, if the user leaves the workstation.
- Using file attributes such as read-only and hiding.
- Encrypting data.

Security threats and control measures

Threats

1. Viruses

These are malicious programs that are designed to cause harm to the computer systems data information and programs. Types of viruses include; file virus, worms, Trojan horses and root kits.

i) File virus: It launches itself when the file is opened and destroys the contents.

ii) Worm: It is a malicious program that replicates itself and fills computer idle memory.

iii) Trojan horse: It is a program that alleges to be useful to the computer but instead performs illegal activities such as introducing a virus. iv) Root kit: It is a group of malicious computer software, designed to allow access to a computer area that is not permitted and often hides its existence or that of other programs.

Characteristics of a computer infected by a virus

- It takes longer time to startup or boot.
- Hangs more often during operation.
- Applications take long to load.
- Unwanted random messages popping up on the screen.
- Disabling peripheral devices.
- Drives not in use getting accessed.
- Files disappearing mysteriously.
- Change of file names and space occupied.
- Reduced file size, encryption of files, loss of data etc.

2. Logic bomb

2. Logic bomb

Is an instruction secretly incorporated in a program so that if a given condition is satisfied its harmful effect occurs.

3. Unauthorised access

It refers to illegal access to computer systems or websites.

4. Computer errors and accidents

A computer error is any problem that occurs unexpectedly that causes a computer to malfunction. These errors can be hardware, software oriented or human error.

5. Theft

This includes stealing computer based information or computer accessories for malicious reasons.

6. Natural disaster

These are calamities that are beyond human control such as floods, earthquakes, lightening among others.

Control measures

Control measures against virus

- Running up-to-date anti-virus software programs regularly.
- Restricting movement of removable storage devices in and out of the organisation.
- Disabling the drive for rewritable media.
- Avoid opening e-mail attachments before scanning them.
- Scanning file attachments before opening them.
- Avoid responding to popup messages.

Functions of antivirus software

- Prevents or protects virus infections.
- Identify viruses and alerts to the computer users about virus threats.
- Isolates viruses infected files (Quarantine).
- Eliminates viruses (Delete or Destroy viruses).
- Protects files from viruses as the computer receives them.
- Forwarding the suspected viruses' patterns to antivirus developers for analysis.

Control measures against unauthorised access

1. Use of passwords – Is a security measure consisting a combination of characters which may include, numbers, letters, special symbols. One needs to change the passwords regularly to ensure security of the data. They should have a minimum of six characters.
2. Firewall.
3. Employing security guards or dogs.
4. Locking the computer room.
5. Access level or user groups privileges.

Control measures against theft

Physical security means physical restriction to the computer system area by use of security guards, burglar proofing, alarms and dogs. Control measures against computer errors

- Proper vetting of employees contracted.
- Limiting access to computer systems.
- Access levels or user groups privileges.
- Performing frequent system auditing.
- Using Uninterrupted Power Supply (UPS) backup.
- Training users on the importance of good practices in using systems.

Control measures against natural disaster

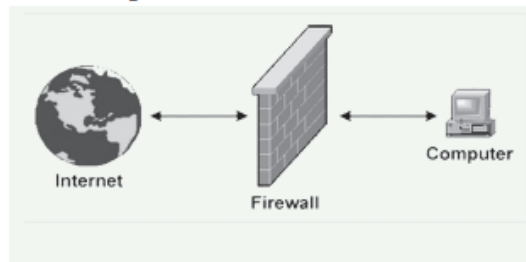
- Having backups of data in regions away from the computer center.
- Using protective safes against fire, water among others.
- Use of lightning arrestors in the prone areas to avoid fire from lightning.
- Installing computers in raised grounds to be safe from floods.

Computer crimes

- **Trespass** - Illegal physical entry to restricted places where computer hardware, software and backed up data is kept.
- **Hacking** - Breach of security codes and passwords to gain unauthorised access to a computer system using software.
- **Tapping** - Illegal acquisition of data on transit over a communication media.
- **Cracking** - Use of guesswork repetitively in order to gain access through weak access points.
- **Piracy** - Illegal copying of software whether for personal use or re-sale.
- **Fraud** - Illegal access to data and making changes to that data e.g. changing bank account.
- **Sabotage** - This is destruction of computer components by disgruntled employees rendering the system useless thus crippling the operations of an organisation.
- **Eavesdropping** - It is secretly listening, recording, transmitting any communication without the owners' consent.

Detection and protection against computer crimes

- **Audit trail:** It is used to keep a record of all the activities of a computer system which can be used to track down the usage of the system.
- **Data encryption:** Scrambling up of messages or data into a form that cannot be read without decrypting or deciphering it during transit in the medium.
- **Log files:** A file that keeps and lists events that happened in a computer system such as web servers maintain log files listings every request made to the server.
- **Firewall:** A firewall is a hardware or software that filters information coming in and going out of an individual/organisations' network.



Laws governing protection of information systems

- a) Data belonging to a person should not be released to other persons without permission from the owner.
- b) Data and information should be secured against loss or exposure.
- c) Data and information should be availed when needed.
- d) Data and information should be correct and updated.
- e) Data and information collected should be used for legitimate goal.

KCSE Revision Questions

KCSE 2006 Paper 1

Qn.19. c) Describe the following term with respect to computer security: i) Logic bombs

KCSE 2006 Paper 1

Qn.19. d) List three functions of antivirus software. (3 marks)

KCSE 2010 Paper 1

Qn.19. a) Explain how data in a computer system is secured using:

- i) Password
- b) State three characteristics of a suitable password.
- c) State two characteristics of a computer that is infected by computer viruses.

KCSE 2009 Paper 1

Qn.1. Give a reason for each of the following:

- a) Changing a password regularly;
- b) Typing and re-typing a new password when changing it.

KCSE 2007 Paper 1

Qn.6. You have been asked to change your computer password. State a precaution you need to take in order to avoid each of the following:

- a) Forgetting the password
- b) Hacking

KCSE 2016 Paper 1

Qn.20. Explain three ways in which an operating system provides data security in a computer system. (6 marks)

KCSE 2007 Paper 1

Qn.11. A computer technician found it necessary to disable a firewall when working on a computer system. State two reasons that may have necessitated disabling of the firewall. (2 marks)

KCSE 2007 Paper 1

Qn.3. Pesa Tele Company has offices in Nairobi and Kampala connected in a network. The management is convinced that someone is illegally gaining access to the data in their computers. State three ways in which the company will overcome this problem (3 marks) KCSE 2006 Paper 1

Qn.19. c) Describe the following terms with respect to computer security:

- i) Physical security (2 marks)
- ii) Tapping (2 marks)