



# *Data security and controls*



# Introduction

- The growth and widespread use of information and communication technology has contributed to the rise in *cybercrime, terrorism, violation of privacy and political crises* in some countries
- To minimise these negative effects, there is need for better methods of protecting computers, data and confidential information

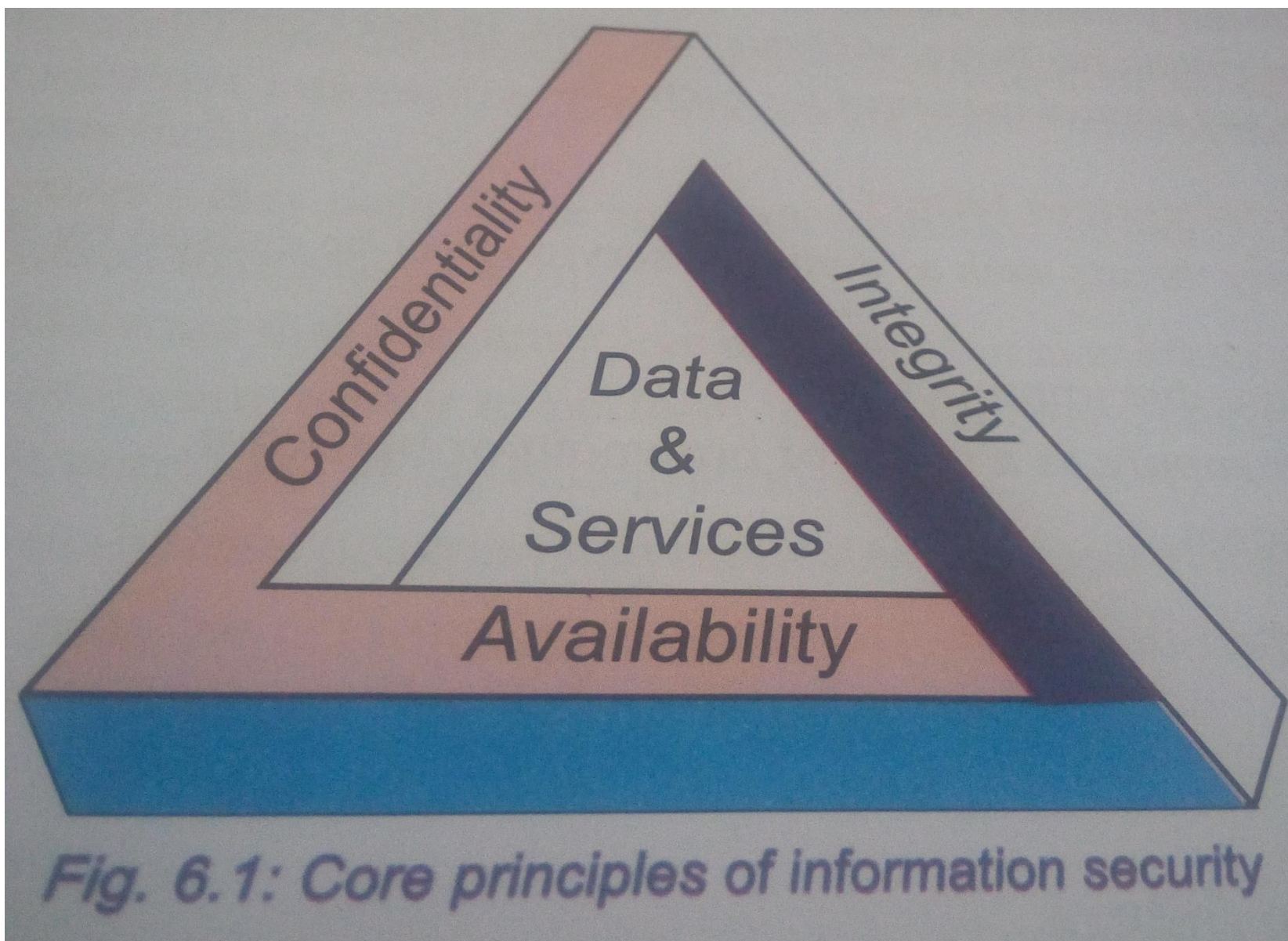



# Definition of terms


- **Data** – these are raw facts, letters, numbers or even graphics that are yet to be processed
- **Data security** – this is protection of data or programs against threats that may lead to either loss data, integrity and confidentiality
- **Data control** – refers to all possible measures taken to ensure security of data, information or programs

# Data security core principles

- The three core principles of data security also referred to as information security are **Confidentiality, Integrity** and **Availability** as shown in CIA Triad diagram figure 6.1 below.



- 
- **Confidentiality** – means that sensitive data or information belonging to an individual, organisation or government should not be accessed by or disclosed to unauthorised people. Eg employee details, classified military information, financial records and health records
  - **Integrity** – means that data should not be modified without owner's authority. Data integrity is violated when a person accidentally or with malicious intent erases or modifies important files such as pay roll or a customer's details.

- 
- ***Availability*** – information must be available on demand. This means that any information system and communication link used to access it must be efficient and functional. An information system may be unavailable due to power outages, hardware failures, unplanned upgrades or repairs.

# Difference between private and confidential data

- **Private data** – refers to data or information that belongs to an individual and must not be accessed by or disclosed to any other person unless with direct permission from the owner. Eg pin no, passwords, login details
- **Confidential data** – this is data or information held by a government or organisation about people. The data must be protected against unauthorised access or disclosure. Eg bank details of customers held by banks,





# Security threats and control measures

## 1. Threats from Viruses and other malicious programs

- A computer virus is a destructive program that attaches itself to other files and installs itself without permission on the computer when the files are opened for use.



# Types of Computer Viruses

- Boot Sector – they destroy the booting information on storage devices.
- File Virus – attach themselves to files.
- Hoax Virus – come as e-mail with an attractive subject and launches itself when e-mail is opened.
- Trojans – they perform undesirable activities in the background without user knowledge.
- Worms – it sticks in the computer memory.
- Back doors – may be a Trojan or Worm that allows hidden access to a computer system.



# Sources of viruses

- Contact with contaminated systems.
- Pirated software.
- Infected emails
- Infected proprietary software.
- Freeware and shareware.
- Updates of software distributed via networks.



# Virus symptoms

- Unfamiliar graphics.
- Programs taking long to load.
- Unusual error messages occurring more frequently.
- Less memory available than usual.
- Files/Programs disappearing mysteriously.
- Changes to disk volume IDs.
- Disk access seems excessive for simple task.



# Control measure against Virus

- Install the latest version of anti-virus software on the computers. Eg AVG, Norton, NOD32, MacAfee among others
- Always scanning removable storage media for viruses before using them.
- Always back up important files or programs to avoid losing them.
- Avoid opening mail attachment before scanning them for virus.
- Avoid buying pirated software



## 2. Threats from system failure

- Security of data may fail due to the following system related problems:
  - i. Hardware failure due to improper use
  - ii. Unstable power supply as a result of brownout or blackout
  - iii. Network failure
  - iv. natural disaster
  - v. Storage failure



# Measures against system failure

- Computer systems should be connected to surge protectors or UPS
- Organisations should put in place fault tolerant systems with redundant storage, peripheral devices and software
- Put in place **disaster discovery plans** by establishing offsite storage (cloud storage) of an organisation's information assets



### 3. Threats from physical theft

- Some valuable computer software and hardware such as hard disks, whole computer systems may be stolen by people with malicious intent. These people may be untrustworthy employees of company or outsiders.
- The reason for physical theft may be commercial, destruction to sensitive information or sabotage





# Control against physical theft

- Employ guards to keep watch over data and information centers and backup sites.
- Reinforce weak access points like the windows, doors with metallic grills and secure padlocks.
- Create backups in locations away from main computing Centre.
- Insure the hardware resources with a reputable insurance firms.
- Motivate workers so that they feel a sense of belonging in order to make them trusted custodians of computer resources



# Intellectual theft through piracy

- Software, information and data are protected by *copyright and patent laws*.
- Piracy is a form of intellectual property theft through illegal copying of software, information or data.



# Control measures against piracy

- Make software cheap enough to increase affordability.
- Use licenses and certificates to identify genuine software.
- Set installation password to deter illegal installation of software.
- Enforce laws that protect the owners of data and information against piracy

## 4. Threats from fraud

- Fraud refers to the use of computer to cheat other people with the intention of gaining money or information.
- Fraud is stealing by false pretence
- ☞ Give examples of fraud in contemporary life
- ☞ What are control measures against fraud

## 5. Threat from sabotage

- Sabotage refers to malicious destruction of data and information with the aim of crippling service delivery, or causing great loss to an organisation.
- Sabotage is usually carried out by disgruntled employees or competitors with the intention of causing harm to the organisation
- ☞ What are control measures against sabotage



## 6. Threats from computer errors and accidents

- Errors and accidental access to data and information may be as a result of people experimenting with features they are not familiar with. Also people might make mistake by printing sensitive reports and unsuspecting give them to unauthorised person.



# Control Measures against computer errors and accidents

- Use error recovery tools provided by windows operating system
- Back up data periodically so that in case of any accident, the back up can be used.
- Use unformatted utilities. This utility enables one to recover data and information for a formatted computer eg *data scavenger program*
- Use the recycle bin to recover temporary deleted files




## 7. Threats to privacy and confidentiality


- Private and confidential data must be protected against unauthorised access or disclosure.



## Computer crimes (cyberterrorism) that may compromise data privacy or confidentiality

- ❖ **Eavesdropping** – this is tapping into communication channels to get information. It is mainly done by hackers and crackers
- ❖ **Surveillance (monitoring)** – refers to monitoring use of computer systems and network using background programs such as *spyware and cookies*. The information gathered may be used for malicious activities such as propagating propaganda or sabotage.
- ❖ **Industrial Espionage** – this is spying on a competitor to get information that you can use to counter or cripple the competitor

- 
- ❖ **Social engineering** – this refers to the act of soliciting for sensitive information from unsuspecting users to carry out some malicious activities on their information and information systems eg
  - ❖ **Alteration** – this is illegal modification of private and confidential data and information with the aim of misrepresenting facts
  - ❖ **Trespass** – this refers to illegal access to the computer lab as well as data sent over network

- 
- ❖ **Hacking and cracking** – a hacker is a person who gains unauthorised access to information for fun by breaking passwords or finding weak access points to software systems while a cracker gains unauthorised access for malicious reasons


### **Reasons/motivation for hacking**


- Some people like software challenges and feel great after hacking a system
- Hackers are commercially hired by software manufacturers to test the security level of a new software system. This form of evaluation is called **penetration testing**.



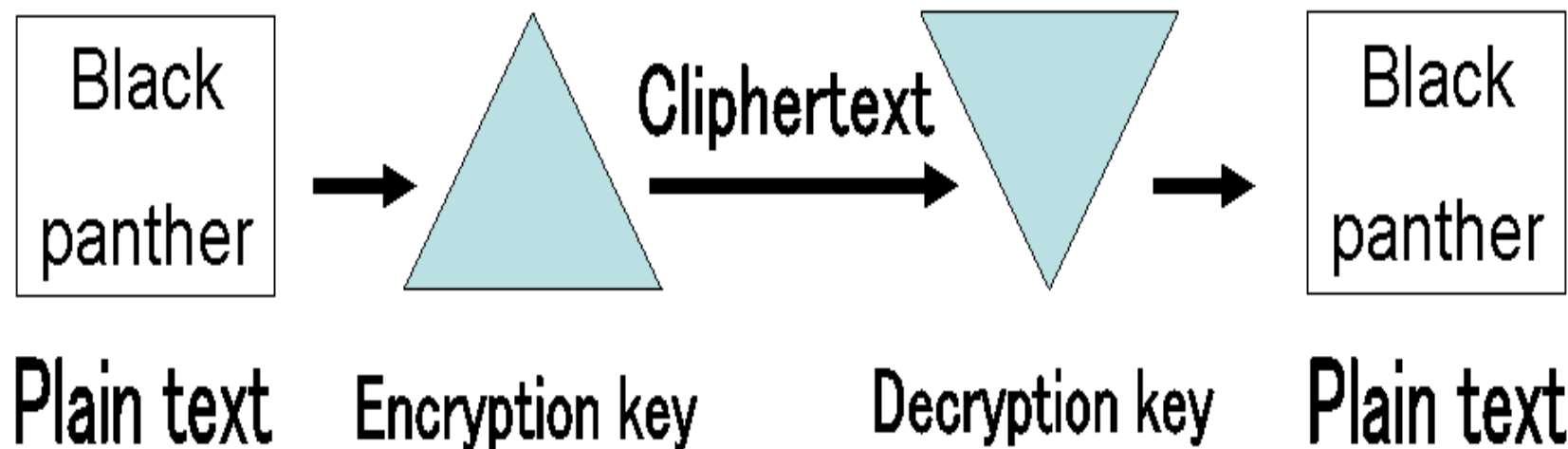
## Detection and prevention against computer crimes and unauthorised access


- **Carry out an Audit Trial** – this refers to careful study of an information system by experts to identify any loophole that can be used to illegally access the system.
- **Use of firewalls** – a firewall is a device or software system that filters the data and information exchanged between different networks by enforcing the host network access control policy. Firewall monitor and control access to and from protected networks.

- 
- **Use of Log Files** – they are special system files that keep a record (log) of events on the use of the computers and resources of the information system. The information system administrator can therefore easily track who accessed the system, when and what they did on the system.

- 
- **Data encryption** – this is the process of changing data before transmission or storage in the form that cannot be read by unauthorised users.
  - ➔ *The message to be encrypted is called plain text, the encrypted data sent over network is called ciphertext.*
  - ➔ *On the receiving side, the receiver needs a decryption key to decrypt data*

# The process of encrypting and decrypting text



- 
- **Biometric security** – this is a form of unauthorised control measure that takes the user's attributes such as voice, fingerprints and facial recognition. Eg
  - **Patch** – this is a line of code which repairs the defect in software without interrupting its proper operations. Eg automatic security updates
  - **Other access control measures** – access control can be enhanced by implementing multi-level authentication policies such as: assigning users log on accounts, smartcards and PIN





# Difficulty in detection and prevention of computer crimes

- The crime might be complex.
- It's not easy to find clear trail of evidence leading to the guilty party e.g. No finger prints.
- There are no witness.
- Few people in management and law enforcement know enough about computers to prevent the crime.



# General Laws governing protection of information

- Data and information should be kept secure against loss or exposure.
- Data and information should not be kept longer than necessary.
- Data and information should be accurate and update.
- Data should not be transferred to other countries without the owner's permission.
- Data and information should be collected, used and kept for specified lawful purposes.