Form two 2016 April holiday assignment. Read and make notes on the topic: Data Security and Controls

DATA SECURITY AND CONTROLS

DATA SECURITY AND CONTROLS

Specific Objectives

By the end of the topic the learner should be able to:

1. Define the terms data security and privacy
2. identify security threats on ICT and possible control measures
3. identify types of computer crimes
4. discuss laws governing protection of information and communication technology systems

Contents

Definition of data security and privacy
Security threats and control measures

- Threats e.g.

1. Virus
2. Unauthorized access
3. Computer errors and accidents
4. Theft

- Control measures e.g.

1. anti virus software
2. password
3. user access levels
4. backups

- Computer crimes e.g.

1. Trespass
2. Hacking
3. Tapping
4. Cracking
5. Piracy
6. Fraud
7. Sabotage
8. Alteration

- Detection and protection e.g.

1. Audit trail
2. Data encryption
3. Log files
4. Firewalls

- Laws governing protection of information systems

Introduction

- Due the rapid growth and widespread use of information and communication technologies, Internet services as well as numerous occurrences of international terrorism, demands better methods of protecting computers, data and information.

Definition

Data security is the protection of programs and data in computers and communication systems against unauthorized modification, destruction, disclosure or transfer whether accidental or intentional.

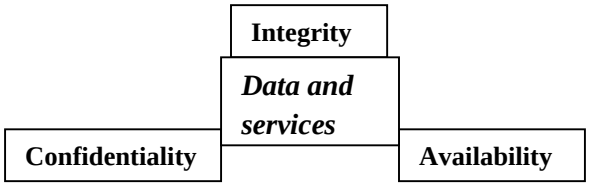
Data control

It is the measures taken to enforce the security of the programs and data.

Data can be lost in various ways, such as viruses, user errors, computer crashes, hacking etc. In order to protect against data loss, controls need to be put in place.

Data Security Core Principles

The three core principles of data security also referred to as information security are confidentiality, integrity and availability. Below is CIA Triad diagram.



Confidentiality

- It means that sensitive data or information belonging to an organization or government should not be accessed by or disclosed to unauthorized people. Such data include employees' details, classified military information, business financial records etc.

Integrity

- This 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 payroll or a customer's bank account file.

Availability

- The 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.

Definition of other terms:

Form two 2016 April holiday assignment. Read and make notes on the topic: Data Security and Controls

Vulnerability: weakness in the system that can be compromised and therefore lead to loss or harm e.g. weak password.

Threats: circumstances that have the potential to cause loss or harm. Types of threats include: Interception, Interruption, Modification, and Fabrication.

Authentication: It is the verification of the identity of the user. It is achieved through; - something you know i.e. password, use what you have i.e. badge, smartcard, something that you are e.g. biometric analysis i.e. finger prints, voice recognition, retina, face recognition etc.

Denial of service

Denial of service (DoS) usually refers to an attack that attempts to make a computer resource unavailable to its intended users by flooding a network or server with requests and data.

Non – repudiation

In the field of computer security, the term **nonrepudiation** means:

> " the assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. "

> " [a] service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified and validated by a third party as having originated from a specific entity in possession of the private key (i.e., the signatory).[2] "

> " [a] technique used to ensure that someone performing an action on a computer cannot falsely deny that they performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.[3] "

Non-repudiation provides protection against an individual falsely denying having performed a particular action. It provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. For example, non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document.

A mechanism that provides a non-repudiation service is a digital signature combining public key cryptography and a timestamp with the message to be secured.

SECURITY THREATS AND CONTROL MEASURES

Some of the security threats include: - viruses, unauthorized access (hacking), computer errors and accidents, theft.
Security threats to computer-based information systems, private or confidential data include unauthorized access, alteration, malicious destruction of hardware, software, data or network resources, as well as sabotage.
The goal of data security control measures is to provide security, ensure integrity and safety of an information n system hardware, software and data.

a. Information system failure

Some of the causes of computerized information system failure include: -

i. Hardware failure due to improper use.
ii. Unstable power supply as a result of brownout or blackout and vandalism.
iii. Network breakdown
iv. Natural disaster

v. Program failure

Control measures against hardware failure

i. Use UPS and surge protectors to protect computers against brownout or blackout which may cause physical damage or data loss.
ii. Use disaster recovery plans which involve establishing offsite storage of an organizations database so that in case of disaster or fire accidents, the company would have backup copies to reconstruct lost data from.

b. **Threats from malicious programs (Viruses**).

A virus – is a destructive program that attaches itself on removable drives and causes damage to a computer system such as deleting system files, data and application files.

The malicious programs may affect the smooth running of a system or carry out illegal activities. Some of the common types of malicious programs include: -

i. Boot sector viruses – they destroy the booting information on storage media.
ii. File viruses – attach themselves on files
iii. Hoax viruses – come as e-mail with attractive messages and launch themselves when e-mail is opened.
iv. Trojan horse – they appear to perform useful functions but they are carriers of viruses. Trojan horses may come inform of games and screen savers.
v. Worms – this is a malicious program that self-replicates hence clogs the system memory and storage media.
vi. Backdoors – may be a Trojan or a worm that allows hidden access to a computer system.

Symptoms of virus on a computer system

i. Unusual and frequent error message.
ii. Loss or change of data
iii. System crash
iv. Programs loading slowly from the normal operation.
v. Slow-down of the general system.
vi. Missing files or folders.
vii. Your application crashes or hangs when opening documents.

Ways through which viruses get into the system: -

1. Copies of software (including games), especially with illegal copies.
2. Downloading and opening of infected files from the internet
3. Opening infected files received through e-mails.
4. Hackers' intent on malicious destruction of networked systems to which they have gained unauthorized.
5. Through freeware/shareware and bulletin board programs that have not been checked for viruses.
6. Exchange and use of infected floppy diskettes, flash disks etc from one computer to another.

Control measures

i. Always scan removable storage media for viruses before using them.
ii. Scan mail attachments for viruses before opening or downloading an attachment.
iii. Install the latest versions of anti-virus software on the computers. Make sure that you continuously update the anti-virus software with the new definitions to counter the new viruses.
iv. All software and data files should be backed up regularly. File backup can be used to restore lost files in the event of system failure.
v. If you are using Microsoft applications, ensure that the Macro Virus Protection is enabled.
vi. Use an operating system such as UNIX which has security features that protect computers from many of the traditional viruses.

c. Physical theft and system crashing

Data and information can be lost if computer are stolen or the hardware crashes. Currently many cases of people breaking into an office or firm and stealing computers, hard disks and other valuable computer accessories. This may be done by untrustworthy employees of firm or by outsiders

Control measures against theft

1. Employing security agents to keep watch over information centers and restricted backup sites.
2. Reinforcing weak access points like the windows, door and roofing with metallic grills and strong padlocks.
3. Motivating workers so that they feel a sense of belonging in order to make them proud and trusted custodians of the company resources.
4. Insure the hardware resources with a reputable insurance firm.

d. Hacking

Form two 2016 April holiday assignment. Read and make notes on the topic: Data Security and Controls

It is when an individual gets unauthorized access into a computer system.
Control measures against hacking

1. Logging off correctly from the computer when one is leaving the machine.
2. Choosing of passwords that are not obvious. They should at least six characters, a mixture of characters and numbers and both upper and lower case letters.
3. Keeping passwords confidential and not writing them down anywhere.
4. Changing of passwords frequently.
5. Encrypting data that is transmitted using the telecommunications network or wireless communication.
6. For highly sensitive data, such as military intelligence where the password protection is not enough, using other methods of authenticating users, such as fingerprints, voice recognition etc.

e. Computer errors and accidents

A computer error is the occurrence of an incorrect results produced by the computer. They can be caused by: -

i. User errors such as incorrect entry of data values, or pressing the wrong keys.
ii. Users accessing files or parts of an application that they are not supposed to.
iii. Program bugs – errors in the logic of the program

Control measures against computer errors and accidents

i. Users to be trained to use applications properly in order to minimize data errors.
ii. Computer programs should be made user-friendly so that any errors are trapped and the user has a chance to correct them.
iii. The software to be tested thoroughly to ensure that it is bug-free.
iv. User Access Levels should be properly defined to ensure that users do not accidentally or purposely access files or data that they are not authorized to access.

COMPUTER CRIMES

A computer crime occurs when a computer is used in some way to perform an illegal activity.
Examples include:

i. Trespass
ii. Hacking and Cracking
iii. Tapping
iv. Piracy
v. Fraud
vi. Sabotage
vii. Alteration

Software Piracy

- It is a form of intellectual property theft i.e. illegal copying of software, information or data with the intention of selling or using them without owners' permission. Software, information and data are protected by copyright and patent laws. For example music industry is worst hit by these illegal deals which entails unauthorized copying of songs.

Types of software piracy include:

a. Licensed-user duplication for unlicensed users.
b. Pre-installed software
c. Internet piracy
d. Counterfeiting

Control measures include: -

i. Enforcing laws that protect the owners of data and information against piracy.
ii. Making software cheap enough to increase affordability.
iii. Using licenses and certificates to identify original software.
iv. Setting installation passwords that deter illegal installation of software.

Fraud

- With the dynamic growth of Internet and mobile computing, more sophisticated cyber crimes like fraud are on the rise. Fraud is stealing by false pretense.
- Fraudsters can be either employee's in a company non-existent company that purports to offer Internet services such as selling vehicles etc. For example the Pyramid Scheme in which many Kenyans were conned.

Other forms of fraud may also involve computerized production and use of counterfeit documents.

THREATS TO PRIVACY AND CONFIDENTIALITY

- Privacy means that data or information belonging to an individual should not be accessed by or disclosed to other people. It is an individual's right to determine for themselves what should be communicated to others.

Form two 2016 April holiday assignment. Read and make notes on the topic: Data Security and Controls

- Confidentiality on the hand means that sensitive data or information belonging to an organization or government should not be accessed by or disclosed to unauthorized people.

Private and confidential data must be protected against unauthorized access or disclosure.
Examples of computer related crimes that compromise data privacy or confidentiality include: -

Eavesdropping

- It is the act of secretly listening to the private conversation of others without their consent. OR it refers to tapping into communication channels to get information.
- Hackers mainly use eavesdropping to access private or confidential information from Internet users or from poorly secured information systems.

Computer Surveillance

- Surveillance refers to monitoring use of computer systems and networks using background programs such as spyware and cookies. The information gathered may be used for one reason or the other e.g. spreading propaganda or sabotage.
- It may also involve accessing the storage mechanism of an individual's computer or monitoring an individual's operation of a computer in most cases without their knowledge. This can be achieved by both hardware and software methods.
- Hardware method involves use of keylogging or ***keystroke logging***. A hardware key logger is a device that plugs in between your keyboard and your computer.
- A software method involves use of ***spyware***. The software is usually installed secretly on a computer, covertly (secretly) monitors the user's actions without his or her knowledge. It can save its findings locally or transmit them to someone else.

- Spyware is a type of malware that is installed on computers and collects information about users without their knowledge. The presence of spyware is typically hidden from the user.
- Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spywares such as keyloggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users.
- While the term spyware suggests that software that secretly monitors the user's computing, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity.
- Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs. In an attempt to increase the understanding of spyware, a more formal classification of its included software types is captured under the term privacy-invasive software

Industrial Espionage

- It involves spying on a competitor to get information that can be used to cripple the competitor.
- It is when confidential information from within companies and other commercial organizations is obtained by spying, in an effort to gain some advantage to the detriment of the body being spied on. They can be employees who are on the verge of leaving or on-site contractors.

Hacking and cracking

- Hacking is the unauthorized accessing of a computer system.
- A hacker is a person who gains unauthorized access to information just for fun, while a cracker gains unauthorized access for malicious reasons.
- Hackers and crackers violate the security measures put in place such as by passing passwords or finding weak access points to software.

Methods hackers use to gain access to computers are:

a. Impersonation – pretending to be someone who is a legitimate user.
b. Brute force attacks – trying every possible combination of characters to find the password.
c. Remote login – using the flows in operating systems to find a back door that allows a hacker to connect to a remote computer and control it.

Alteration

- It is the illegal modification of private or confidential data and information with the aim of misinforming users. It is usually done by people who wish to conceal the truth or sabotage certain operations.
- Alteration compromises the integrity of data and information making it unreliable.

Sabotage

- It involves destroying or altering of data in the computer system that would otherwise be critical to the organization.
- The organizations employees may be dissatisfied with the current running of the organization and may resort to sabotage. They can even destroy computer systems containing sensitive information that the organization depends on for its business survival.

NB:

Form two 2016 April holiday assignment. Read and make notes on the topic: Data Security and Controls

For fun
Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find leapers fun and admit swordfish rank overwhelmingly anyday.

Solution:
Send lawyers gun and money.

Dear Bob,
Greetings to all. Many thanks for your
Letter and for the enclosed exam package
All entry forms and fees should be ready
for dispatch on Friday
20th or at the very least, am told the 21st
admin has improved considerably although there is room
for further improvement still, just give us two or three
more years and will really show you! Please
don't let the wretched proposals destroy
your basic Q and A pattern. Certainly this
sort of change will bring chaos if implemented immediately.
Regards John.

Solution:
Bob your package ready Friday 21st room three. Please destroy this immediately. John

Sample Nth Letter Code Paragraph
Coded Message: Every 10th Letter
I was just thinking how everything looks funny painted on. I'm lying here enjoying my innocent play day and I am wondering, "Before this, everything in a life meant something else. I feel hot sometimes and cold all over some days." I feel change will be here soon. Or maybe I am being silly. Is that weird? Eh, who knows! Nothing can do anything here. I may see someone at lunch time. I plan to call!
Decoded Message:
HELP ME I AM BEING HELD HERE SEND HELP
Sample Acrostic Code Paragraph
Coded Message: First Letter of Sentence Acrostic
Hello! Everything is going fine. Lots of things to do! Please remember to feed my fish. Maybe you can send a picture. Everyone here has been nice. I wish you could meet them. Anyway, something funny happened the other day. My foot got caught on a log and I tripped. But the funniest part was when a bird pooped on my head. Everyone laughed at that. I couldn't believe it myself. No one warned me there was a big log in front of me. Gotta make sure to look out!
How has everything been for you? Everything okay? Little by little, I am learning how to camp. Doing everything for myself has been fun. Have you started school yet? Enjoying your classes? Remember to pay attention! Everyone would tell you that trick!
So, I guess that's it for now. Everyone says hi. No need to send anymore clothes. Doing laundry in the lake has been fun. Hope everything is going well for you! Every day I miss you. Lots of love. Please say hi to everyone!
Decoded Message:
HELP ME I AM BEING HELD HERE SEND HELP
Sample Pig Paragraph
Pig Coded Message:
Lup e a rup nup i nup gup tup o sup pup e a kup Pup i gup i sup e a sup yup wup i tup hup pup rup a cup tup i cup e. Mup e sup sup a gup e cup o dup e sup a rup e hup e lup pup fup u lup fup o rup wup hup e nup yup o u wup a nup tup tup o cup o mup mup u nup i cup a tup e sup e cup rup e tup lup y. E vup e nup tup hup e mup i lup i tup a rup y u sup e sup cup o dup e sup a nup dup cup i pup hup e rup sup i nup cup a sup e tup hup e i rup mup e sup sup a gup e sup a rup e i nup tup e rup cup e pup tup e dup bup yup tup hup e e nup e mup y. I fup e xup e cup u tup e dup cup o rup rup e cup tup lup yup, a nup yup o nup e cup a nup cup o mup mup u nup i cup a tup e wup i tup hup cup o mup pup lup e tup e pup rup i vup a cup yup.
Decoded Message:
Learning to speak Pig is easy with practice. Message codes are helpful for when you want to communicate secretly. Even the military uses codes and ciphers in case their messages are intercepted by the enemy. If executed correctly, anyone can communicate with complete privacy.
Keyboard Cipher

Form two 2016 April holiday assignment. Read and make notes on the topic: Data Security and Controls

Get a keyboard, and make sure that it has all 26 letters of the alphabet. This is recommended if you are typing your message on the computer. You will need a Qwerty type because keyboards from different countries will have different letters.
The keyboard is kind of like the St. Cyr. Slide. However, the alphabet on the keyboard (locations) are different from plain alphabet. You can shift the keyboard to one letter space to the left, so on your keyboard, H becomes G, F becomes D, and A becomes L ("turn over to the other side"). For example, if you wanted to write "Call me as soon as possible," you would type it like this: xlkk nw la aiin la oiaauvkw.

Control measures against unauthorized access

To safeguard data and information against unauthorized access, the following measures should be put in place: -

Using software-based data security:

- Passwords for the system.
- Passwords for individual files or folders.
- Audit trails or access logs.
- Encryption

Anti-virus:

A special type of software used to remove or inactivate known viruses from a computer's hard disk, floppy disk or memory stick. The program can also scan incoming and outgoing e-mail messages to ensure they do not contain infected data. It should be updated via the Internet regularly. Failure to do this may render your software infective against new viruses which are created all the time, and which may pose serious risks to your computer system. Examples of antivirus software's include: McAfee, Norton Antivirus, Avira, Kaspersky, AVG, Microsoft Security Essentials etc.

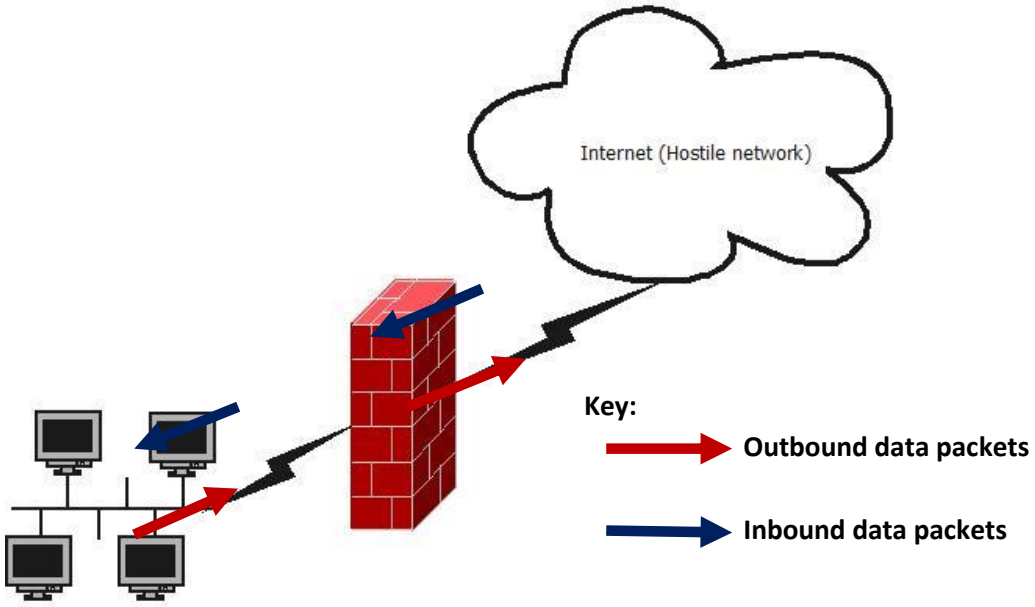
FIREWALL

Definition: -

- They are a set of mechanism that is used to protect a trusted network from a hostile/unsecure network (Internet).
- It is a device or software system that filters the data and information exchanged between different networks by enforcing the host network access control policy.
- They can either be software or hardware. The main aim of a firewall is to monitor and control access to or from protected networks. People who do not have permission (remote requests) cannot access the network and those within cannot access firewall restricted sites outside their network.
- It is possible to have firewalls within organization to protect internal network within an organization i.e. protecting the finance department.

Diagram:

Form two 2016 April holiday assignment. Read and make notes on the topic: Data Security and Controls



Firewalls can protect systems from:
Remote login: - This is when someone is able to connect to your computer and control it in some form, ranging from being able to view or access your files to actually running programs on your computer.
Spam (electronic junk mail): By gaining access to a list of e-mail addresses, a person can send unwanted spam to thousands of users.
E-mail bomb: This is when someone sends you the same e-mail hundreds of thousands of times until your e-mail system cannot accept any more messages.
Viruses: It is a computer program that self-replicates itself in a computer unknown to the victim and destroys or corrupts data.

Advantages of firewall

i. They can stop incoming requests to inherently insecure services, e.g. you can disallow rlogin, or RPC services such as NFS.
ii. They can control access to other services e.g. bar callers from certain IP addresses, filter the service operations (both incoming and outgoing), e.g. stop FTP writes, hide information e.g. by only allowing access to certain directories or systems.
iii. They are more cost effective than securing each host on the corporate network since there is often only one or a few firewall systems to concentrate on.
iv. They are more secure than securing each host due to: the complexity of the software on the host - this makes it easier for security loopholes to appear. In contrast, firewalls usually have simplified operating systems and don't run complex application software, the number of hosts that need to be secured (the security of the whole is only as strong as the weakest link).

Limitations of firewall

i. They do not protect against internal threats such as those caused by disgruntled employees who are likely to be compromised by external hackers.
ii. Cannot protect against virus infected programs
iii. They are a central point for attack, and if an intruder breaks through the firewall they may have unlimited access to the corporate network.
iv. They may restrict legitimate users from accessing valuable services, for example, corporate users may not be let out onto the Web, or when working away from home a corporate user may not have full access to the organization's network.
v. They do not protect against back door attacks, and may encourage users to enter and leave via the backdoor, particularly if the service restrictions are severe enough. Examples of backdoor entrance points to the corporate network are: modems, and importing/exporting floppy discs. The security policy needs to cover these aspects as well. (They cannot protect against attacks that by pass the firewall e.g. using a modem that is not proxy (bypass)).
vi. They can be a bottleneck to throughput, since all connections must go via the firewall system.

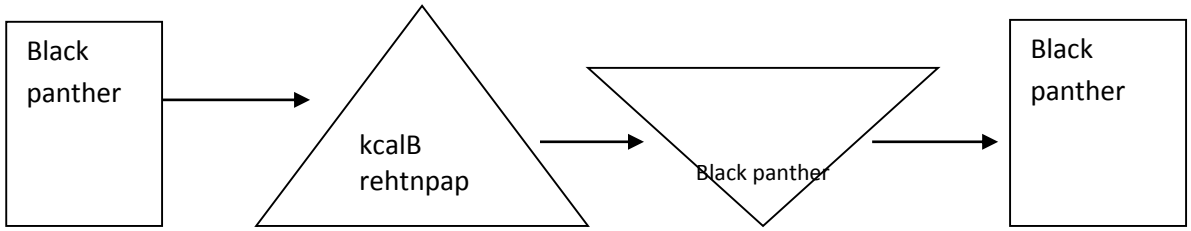
Types of firewalls

i. Packet filtering routers
ii. Proxy gateways
iii. Encryption gateways

Form two 2016 April holiday assignment. Read and make notes on the topic: Data Security and Controls

Data encryption

It is a means of scrambling (or ciphering) data so that it can only be read by the person holding the encryption "key". The key is a secret code that only authorized users share.
Data on transit over a network faces many dangers of being tapped, listened to or copied to unauthorized destinations. Such data can be protected by mixing it up into a form that only the sender and receiver is able to understand.
The message to be encrypted is called the plain text document. After encryption, using a particular order called algorithm or key, the data is sent as cipher text on the network. The recipient receives it and decrypts it using a reverse algorithm to the one used during encryption called a decryption key, to get the original plain text document.
The diagram below indicates the process of encrypting and decrypting text.



Plain text Encryption key Decryption key Plain text

Audit trail

It is a continuous analysis and recording of all the transactions that have been carried out by a computer system in order to exactly pinpoint and identify the sources of the problems.
The transactions are systematically traced for inconsistencies right from the input stage through the output stage.

Security monitors

They are programs that monitor and keep a log file or record of computer systems and protect them from unauthorized access.

i. Biometric security.
It is a growing form of unauthorized control measure that takes the uses' attributes such as voice, fingerprints and facial recognition. For example you can log on swap a finger on a fingerprint swap window.
ii. Other access control measures.
Access control can also be enhanced by implementing multi-level

CONCLUSION

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells.
While some are harmless or mere hoaxes most computer virus are considered malicious.

Worm

Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program. Many people conflate the terms "virus" and "worm", using them both to describe any self-propagating program.

1. Give a reason for each of the following
   (a) Changing a password regularly 1mk
   (b) Typing and re- typing a new password when changing it. 1mk
2. (i) An anti- virus software installed in a computer is loaded into the main memory each time the computer is switched on
   Explain three ways in which computer virus are spread from one computer to another 3mks

(ii) Give two reasons why an anti-virus package should be updated regularly 2mks

3. A student tried opening an application program on a computer that was functioning well. The program did not load and the operating system reported that the memory was insufficient. Give **two** causes of such response. 2mks
4. State **two** measures that can be put in place to control piracy of software. 2mks
5. Pesa Mingi 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 can overcome this problem. 3mks
6. Copyright laws are laws granting authors the exclusive privilege to produce, distribute, perform or display their creative works. It is a legal framework for protecting the works such as book publishing, motion-picture production and recording. State two challenges that are posed to these laws by ICT. 2mks
7. (a) Explain how data in a computer system is secured using: 4mks
   i. Password;
   ii. User access level.
   b. State three characteristics of a suitable password. 3mks
   c. State two characteristics of a computer that is infected by computer viruses. 2mks
8. Define the following terms:
   a. Firewall
   b. Encryption
   c. Impersonation
   d. Audit trail
   e. Eavesdropping
   f. Privacy
   g. Confidentiality
9. Using a diagram, describe how a firewall works.
10. State two merits and two demerits of using a firewall as a control measure.