System Security, ICT ethical Issues and Emerging Technologies

Introduction

The rapid growth and widespread use of information and communication technologies, internet services as well as numerous occurrences of international terrorism, demands betters methods of protecting computers, data and information.

Computer System Security

The three core principles of data security also referred to as information security are confidentiality, integrity and availability.

Confidentiality

Confidentiality 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

Integrity means that data should not be modified without owner's authority. Data integrity is violated when a person accidentally or with malicious intentions erases or modifies important files such as a payroll or a customer's bank account file.

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 failure, unplanned upgrades or repairs.

Security threats and control measures

Security threats to computers-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, ensures integrity and safety of an information system hardware, software and data. In this section, we explore various security threats and control measures for each case.

Information system failure

Some of the cause of computerized information system failure include

1. Hardware failure due to improper use.
2. Unstable power supply as result of brownout or blackout and vandalism.
3. Network breakdown.
4. Natural disaster
5. Program failure

Control measures against hardware failure

Protect computers against brownout or blackout which may cause physical damages or data loss by using surge protectors and Uninterruptible power supply (UPS). For critical systems, most organizations have put into place fault tolerant systems.

A fault tolerant systems has redundant or duplicate storage, peripherals devices and software that provide a fail-over capability to backup components in the event of system failure.

Disaster recovery plans

Disaster recovery plan involves establishing offsite storage of an organization's databases so that in case of disaster or fire accidents, the company would have backup copies to reconstruct lost data.

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.

Confidentiality on the other 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.

Threats from malicious programs

Malicious programs may affect the smooth running of a system or carry out illegal activities such as, secretly collecting information from unknown user. Some of the common types of malicious programs include:

1. Boot sector viruses- they destroy the booting information on storage media.
2. File viruses-attach themselves to files.
3. Hoax viruses- Come as e-mail with attractive messages and launch themselves when e-mail is opened.
4. Trojan Horse- they appear to perform useful functions but instead they perform other undesirable activities in the background.
5. Worms- it is a malicious program that self-replicated hence clogs the system memory and storage media.
6. Backdoors-may be a Trojan or worm that allows hidden access to computer system.

Computer Virus

Computer virus is a destructive program that attaches itself on removable drives and cause damage to a computer system such as deleting system file, data or application files.

How Virus spread on standalone and networked computers

Standalone computer is one which is not connected to any other computer. However networked computer is the one which is connected to any other computer for the purpose of exchanging

data, information or resources. The table below shows how virus spread on standalone and networked computer.

Standalone computer	Networked computer
1. Use of flash disk	1. Through downloading email attachment
2. By using floppy diskette	2. Playing games on internet
3. Transferring files using memory card	3. Downloading files from internet

Control measures against viruses

To protect an information system against viruses:

1. Install the latest versions of anti-virus software on the computers. Make sure that you continuously update the anti-virus software with new virus definition to counter the new viruses.
2. Always scan removable storage media for viruses before using them.
3. Scan mail attachments for viruses before opening or downloading an attachment.

Hacking and cracking

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 a software.

There are various motivations for hacking. One is that some people like the challenge and feel great after successfully hacking a system, while some do it commercially for software manufactures test the security status of a new software system.

Data protection in computer systems

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

Firewall

A firewall is a device or software system that filters the data and information exchanged between different networks by enforcing the host networks access control policy. 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 firewall restricted sites outside their network.

Data encryption

Data on transit over the network faces many dangers of being tapped, listened to or copied to unauthorized destinations. Such data can be protected by mixing up into a form that only the sender and receiver is able to understand. This is by reconstructing the original message from the mix which is called data encryption.

Security monitors

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

Biometric security

Biometric security is a growing form of unauthorized control measure that takes the user's attributes such as voice, fingerprints and facial recognition. For example, you can log on swap a finger on a finger print swap windows.

Password and PIN (Personal Identification Number)

Access control can also be enhanced by implementing multilevel authentication policies such as assigning users log on accounts, use of smart cards and personal identification number (PIN).

Computer Crime

The following are some examples of computer-related crimes that compromise data, information and computer.

Physical theft

The physical theft of computer hardware and software is the most widespread related crime especially in developing countries.

The most common issues now, we here cases of people breaking into an office or firm and stealing computers, hard disks and other valuable computer accessories. In most cases such theft can be done by untrustworthy employees of firm or by outsiders. The reason behind an act may be commercial, destruction to sensitive information or sabotage.

Control measures against theft

1. Employ security agents to keep watch over information centers and restricted backup sites.
2. Reinforce weak access points like windows, door and roofing with metallic grills and strong padlocks.
3. Motivate 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.

Piracy

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

Control measures against piracy

There are several ways of reducing piracy

1. Enforce laws that protect the owners of data and information against piracy.
2. Make software cheap enough to increase affordability.
3. Use licenses and certificates to identify original software.
4. Set installation passwords that deter illegal installation of software.

Fraud

Fraud is stealing by false pretense. Fraudsters can be either employees in a company, non-existent company that purports to offer internet services such as selling vehicles etc. other form of fraud

may also involve computerized production and use of counterfeit documents. This is due to the dynamic growth of internet and mobile computing, sophisticated cybercrimes.

Sabotage

Sabotage refers to illegal destruction of data and information with the aim of crippling services delivery, or causing great loss to an organization. Sabotage is usually carried out by disgruntled employees or competitors with the intention of causing harm to an organization.

Eavesdropping

Eavesdropping 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 system.

Surveillance (monitoring)

Surveillance refers to monitoring use of computer system 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 sabotage.

Industrial espionage

Industrial espionage involves spying on a competitor to get information that can be used to cripple the competitor.

Accidental access

Threats to data and information come from peoples unknowingly giving out information to strangers is or unauthorized persons.

Alteration

Alteration is the illegal modification of private or confidential data and information with the aim of misinforming users. Alteration is usually done by people who wish to cancel the truth or sabotage certain operations.

Alteration comprises the integrity of data and information making it unreliable.

ICT Ethical issues

ICT policy seeks to address issues of privacy, e-security, ICT legislation, cybercrimes, ethical and moral conduct, copyrights, intellectual property rights and piracy.

Information privacy and violation

1. Data should not be disclosed to other people with the owner's permission.
2. Data and information should be kept secured against loss or exposure

3. Data and information should be kept longer than necessary
4. Data and information should be accurate and up to date.
5. Data and information should be collected, used and kept for specified lawful purposes.

Copyrights

Hardware and software are protected by either national or international copyrights, designed and patents laws or act

Emerging Technologies

Concepts of emerging technologies covers the rapid evolution of computers and information technology with the future trends in computer and information and communication technology which is characterized by artificial intelligence and digital forensics.

Artificial Intelligence (AI)

Artificial intelligence refers to a branch of computer science that is concerned with the development of machines that emulate human-like qualities such as learning, reasoning, communication seeing and hearing. Also artificial intelligence refers to the ability of a machine to perform tasks that normally require human intelligence.

Computer scientist and engineers are still working hard to come up with computer reality in near future which can think and learn instead of relying on static programmed instructions.

There are four main application areas of artificial intelligence namely:

1. Expert systems. Software that operate at the level of human expert in specific application.
2. Natural language processing.
3. Artificial neural networks.
4. Robotics/perception systems.

Digital forensics

Digital forensic refers to the forensic science encompassing the recovery and investigation of material found in digital devices often in relation to computer crime.

There are four main application areas of digital forensic namely:

1. Legal consideration- use of digital evidence in court
2. Branches- perception of the computer forensic, mobile device forensic, network forensic
3. Application of digital forensic such as electronic discovery, intrusion etc.
4. Forensic process- analysis and reporting

ICT industry

Information and communication technology (ICT) has created new job titles such as computer operators, computer technicians, system analyst, computer programmers, software engineer,

information systems manager, data base administrator, computer trainer, web administrator, computer graphics designers and network administrator. This section explains some responsibilities of these professionals who are generally called *information technology workers*.

Computer operator

Some of the responsibilities of a computer operator include;

1. Entering data into the computer for processing.
2. 2. Keeping up-to-date records (log files) of all information processing activities.

Computer technician

Given that computers require regular maintenance, upgrading as well as emergency repairs, demand for computer technicians continues to grow as more people computerize their workplaces and homes.

Some of the responsibilities of a computer technician are;

1. Troubleshooting computer hardware and software related problems.
2. Assembling and upgrading computers and their components.
3. Ensuring that all computer related accessories such as printers modems, storage media devices are in good working condition.
4. In developed countries, technicians help hardware engineers in designing and crating some computer components such as storage devices, motherboards etc.

System analyst

This a person who is responsible for analyzing a company's needs or problems then designs and develops a computer based information system.

A good analyst is one who has at least the following attributes;

1. Good problem solving skills and creativity, ie. Must have wide experience in solving problems.
2. Good communication skills: The analyst must be able to communicate clearly and precisely both in writing and in speech. He/she must be able to talk to different groups of people e.g managers, operators, attendant and general public.
3. Must have business knowledge: the analyst must clearly understand the environment for which the system is being developed.
4. Technical knowledge: A system analyst must be well trained in relevant areas of computer science such as hardware, software programing knowledge.

Some of the responsibilities of a system analyst include:

a) Reviewing the current manual or redundant information system and making recommendations on how to replace it with a more efficient one.
b) Working with programmers to construct and test the system.
c) Coordinating training for users of the new system.

Computer programmer

Large organizations such as insurance companies, banks, manufacturing firms and government agents hire programmers to work together with system analysts in order to:

1. Develop in house application programs or system programs.
2. Customize commercial application packages to suite the organization needs.
3. Install, test, debug, and maintain programs developed or customized for the organization.

Computer engineer

Computer and electronic engineers are coming up with new and more efficient technologies in information and communication technology almost daily. Since computers are electronic devices, hardware designers must be good in electronic engineering in order to be able to:

1. Design and develop computer components such as storage devices, motherboards and other electronic components.
2. Determine the electrical power requirement of each component.
3. Re-engineer computer components to enhance its functionality and efficiency.
4. Design and develop engineering and manufacturing computer controlled devices such as robots.

Web administrator/webmaster

Internet is one of the areas of information and communication technology that has drawn the interest of most people. Thus people are able to exchange messages, search for information and do business through the internet.

A web administrator is responsible for:

1. Developing and testing websites.
2. Maintaining, updating and modifying information on the website to meet new demands by the users.
3. Monitoring the access and use of internet connection by enforcing the security measures.
4. Downloading information needed by an organization or institution from internet websites.

Computer graphics designers and typesetters

In publishing, skilled graphics designers and typesetters are required in order to design graphical objects and professional publications. Such people may get employed in publishing houses to typeset books, newspapers and magazines.

Self-employment

Self-employment can be achieved by using a computer or other ICT devices such as mobile phones to start bureau services, internet services, consultancy services and computer hardware and software vendor business.

Network administrator

A network administrator is a specialist whose responsibilities are to:

1. Set-up a computer network.
2. Maintain and enforce security measures on the network.
3. Monitor the use of network resources.
4. Maintain and troubleshoot network related problems.

Computer sales representatives

Computer sales representative should have good knowledge in information and communication technology. This would help them to analyze customer needs and advice accordingly. A good computer salesman needs to be self-confident, persuasive and proficient in business communication.