NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF MANAGEMENT SCIENCES

COURSE CODE: ACC 301

COURSE TITLE: INFORMATION AND COMMUNICATION TECHNOLOGY I

COURSE MATERIAL DEVELOPMENT

ACC301

INFORMATION AND COMMUNICATION TECHNOLOGY I

MAIN CONTENT

COURSE DEVELOPER/ WRITER: ICAN STUDY PACK

COURSE ADAPTER: ADEGBOLA, EUNICE ABIMBOLA
NOUN

COURSE EDITOR: Dr(Mrs) A. O. Fagbemi

PROGRAMME LEADER: Dr I. D. Idrisu NOUN

COURSE COORDINATOR: Anthony I. Ehiagwina

COURSE CONTENT

MODULE 1

Unit One: The Computer

Unit Two: Computer Hardware and Software Technologies

Unit Three: The Historical Development of Computers (Generation of Commuters) Electronic Commerce

Unit Four: The Computer Input and Output Devices

MODULE 2

Unit One: The Computer Net Work and Cabling

Unit Two: Computer Network Topology and General E-Commerce

Unit Three: Communications Supported by Information Technology

Unit Four: Electronic Files Transfer/Security

MODULE 3

Unit One: Computer Crime and Abuse

Unit Two: Computer Virus, Worms, and Trojan, the Threat and Prevention

Unit Three: Information System Architecture (Communication Networks)

Unit Four: System Development Life Cycle (SDLC)

MODULE 4

Unit One: System Requirements, Analysis and Design

Unit Two: Establishing System Objectives, Information Requirements and Solution Alternatives

Unit Three: Systems Installation/Implementation and Maintenance

Unit Four: Critical Factors for the Successful Implementation of a Management Information System

MODULE ONE

GENERAL INFORMATION TECHNOLOGY KNOWLEDGE AND CONCEPT

UNIT ONE: THE COMPUTER

UNIT TWO: COMPUTER HARDWARE AND SOFTWARE TECHNOLOGIES

UNIT THREE: THE HISTORICAL DEVELOPMENT OF COMPUTERS (GENERATION OF COMMUTERS) ELECTRONIC COMMERCE

UNIT FOUR: THE COMPUTER INPUT AND OUTPUT DEVICES

UNIT ONE: THE COMPUTER

CONTENT

7.0 Reference/Further reading

1.0 INTRODUCTION

A computer can be described as an electronic device capable of receiving data through its input device(s), storing the data in its memory, processing it in its processor and then producing meaningful information through its output devices(s) visually or in written form.

A comparison can then be made with the way human beings process data.

When asked a question, you take in the question through the ear (input), store the question in your memory (mind) you do some mental calculation (processing) and then produce the answer orally or in written form (output), so the process is the same, only with computer, processing is more faster. The classification of computer is done successfully according to data processed/function, size, purpose and technologies.

2.0 OBJECTIVES OF THE UNIT

Upon successful completion of this unit, you are expected to do the following:

- Define and explain a computer.
- Examine the general features of computers
- Discuss the classification of computers according to types, purpose and technology.
- Explain the basic computer hardware layout.
- Analyse the components of the central processing unit (CPU)
- Examine the main computer memory, arithmetic and logic unit (ALU), the secondary storage units and out put unit.

3.0 MAIN CONTENT

3.1.0 DEFINITION OF COMPUTERS

A computer can be defined as an electronic device used in processing data and information. It can manipulate and store data for the user's retrieval. It has capacity to process data to generate information. This data can also be stored for later use or further manipulation.

In addition, a computer is a device that accepts data, processes the data in accordance with a user instruction (program) and generates results. It consists of input, output, storage and processing units. It is a system of functional units that can perform substantial computation, including numerous arithmetic operations and logic operations.

Features of Computers

There are certain attributes that characterize a computer that tend to make it advantageous over other means of data processing. Some of these advantages include:

3.1.1 Speed– Computers are electronic devices and as such, can operate at a fast speed. That makes the computer so fast in operation that in a matter of seconds, it can accomplish what will take human beings days to accomplish.

3.1.2 Accuracy- Computers do not make mistakes as long as they are accurately programmed and to a large extent, not faulty in terms of components. Computers can operate error-free, so they can be trusted to produce accurate results which are very vital to the user. It therefore implies that the output or the results of the processing will normally be achieved based on the original data input to the computers. That informs the popular saying 'garbage in, garbage out, (GIGO)".

3.1.3 Reliability – Just as they are accurate, a computer is reliable and consistent in the information produce by it. Given the same program and same data, the result produced should be the same

at all times. That is why computer –type devices like the microprocessors are introduced into household appliances and automobiles to increase their productivity and reliability. This does not mean that the computer cannot breakdown. When it breaks down, it will not longer be operational as long as downtime is sustained. The amount of time that the computer stays in an inactive condition is referred to as downtime.

3.1.4 Versatility – Computers are versatile. They can be used in many fields. Some areas in which computers can be used include; research, aviation, sales force automation, medicine, accounting, auditing, teaching and learning, designing and manufacturing, entertainment, etc.

3.1.5 Mass storage capability– Computers can store very large amounts of data for long periods of time.

3.1.6 Precision– It is possible to represent information, especially numerical qualities, to any (reasonable) desired degree of magnitude. This quality is very useful in scientific and engineering applications.

3.1.7 Security – Because data and information in computer systems are stored in machine–readable form, they are protected from unauthorized people by the use of passwords or some other forms of identification. It therefore can be said that the computer provides a measure of security for data and information stored on it.

3.2 CLASSIFICATION BASED ON SIZE

A. Mainframe computers

These are very large computers, often filling an entire room. They can store very large amounts of information, perform many tasks at the same time, and communicate with many users at the same time. They are very expensive. Mainframe computers unusually have many terminals connected to them. These terminals look like computers, but are only devices used to send receive information from the main computer (mainframe). The terminals can be located in the same room with the mainframe, but can also be in different rooms, buildings or cities. Most mainframe computers need to be operated by professionals and need to be operated in special environment. See picture below for a mainframe environment.

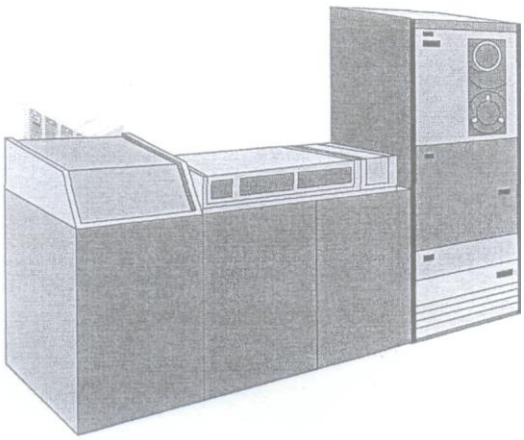


Fig. 1.1. Main frame computer

B. Minicomputers

These are smaller and much less expensive mainframe computers. They posses most of the features found in mainframe computers, but on a more limited scale. That is, minicomputers have many terminals attached to them for users, store tremendous amount of information, but not as much as the mainframe.

C. Microcomputers

These are smaller but most important category of computer systems for end users. They are often referred to as personal computers (PCs).

Microcomputers can further be categorized by size as follows:

- Hands held – Such as PDAs (Personal Digital Assistants), but lack the power of a desktop or notebook computer.
- Notebook – (Laptop) computers are used by people who need the power of a desktop system, and also portability;
- Portable;
- Desktop; and
- Floor –standing

Microcomputers may be used for:

- Office applications
- Personal use; and as a
- Work station (network as an integrated system).

3.2.2 CLASSIFICATION BASED ON PURPOSE

A. General Purpose Computers

This is a machine that is capable of carrying out some general data processing under program control. It is a computer system that can be used to solve different types of problems in different fields. Virtually all computers from micro to mainframe are general purpose computers.

B. Special purpose computers

This is a machine designed to operate a restricted class of problems. An example is computer equipment designed to analyse patient diagnostic problems.

3.2.3 CLASSIFICATION BASED ON TECHNOLOGY

Analog computers

These computers recognize data as continuous measurement of a physical property, such as voltage, pressure, speed and temperature. Examples are thermometer, speedometer, analog wristwatch etc.

Digital computers

These are high speed programmable electronic devices that perform mathematical calculations, compare values and store results. They recognize data by counting discrete signals representing 1 and 0, ON and OFF, high or low, Yes or No etc.

Hybrid computers

These are computers that process both analog and digital data.

3.3 BASIC COMPUTER HARDWARE LAYOUT

The general layout of a digital computer is shown in fig. 1.2. It has an input unit, Central Processing Unit (CUP), output unit and secondary Storage Unit (SSU).

3.3.1 INPUT UNIT

The purpose of the input components of a computer system is to

(i) Accept data in the required form;

(ii) Convert this data into machine-readable form;

(iii) Transmit this data to the central processing unit (CPU).

3.3.2 CENTRAL PROCESSING UNIT (CPU)

This is the unit that does the work of the computer system. It executes computer programs. The program tells the processor (CPU) when and what to read from input unit, what to display or write on the input device, what to solve or retrieve from the secondary storage, etc. This unit is made up of three components, the main memory, the arithmetic and logic unit and the control unit.

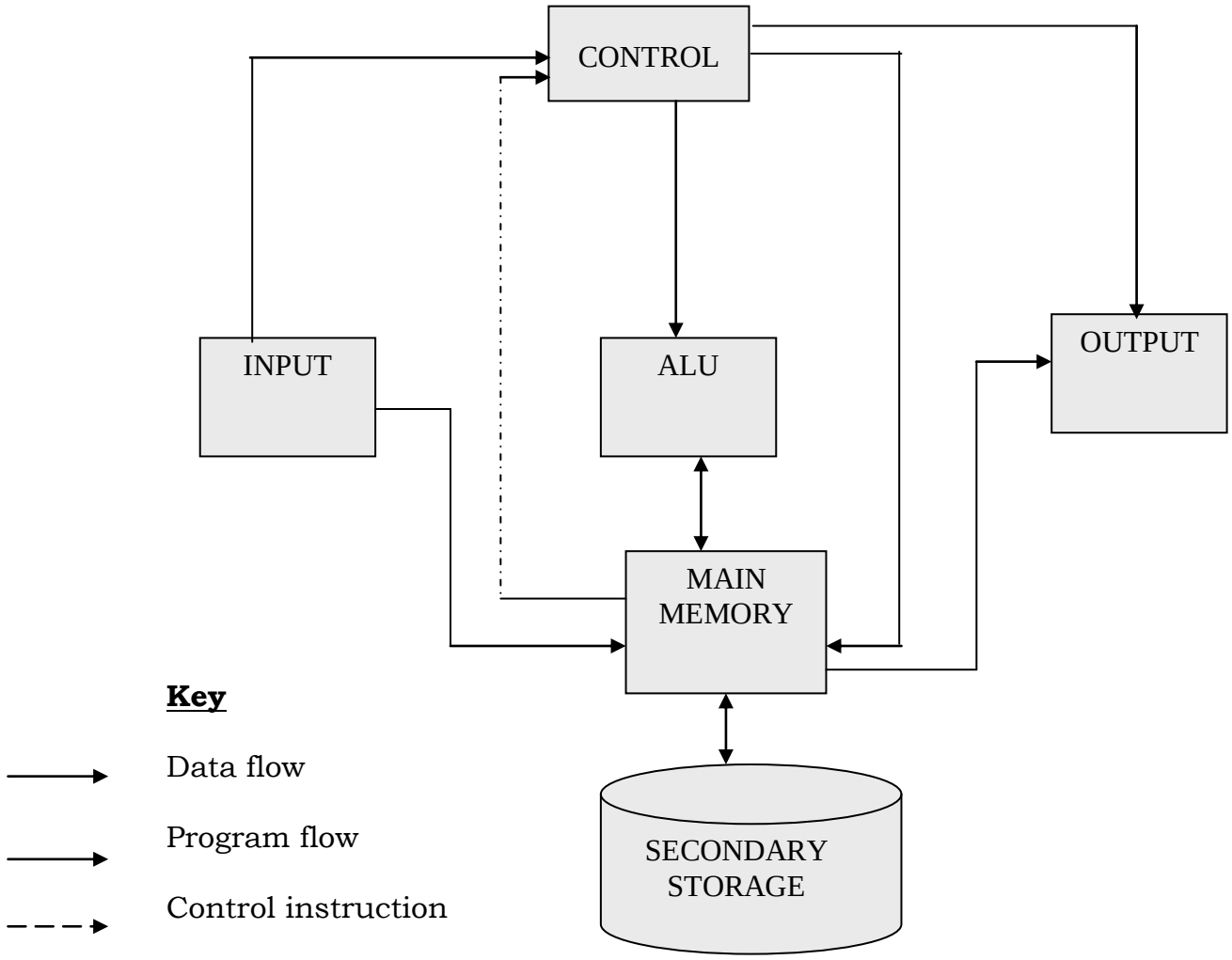


Figure 1.2 General layout of a digital computer

3.3.3 MAIN MEMORY

The purpose of the main memory (also known as Random Access Memory, RAM or Primary Memory or Immediate Access Memory) is to:

(i) Store programs during their execution; and

(ii) Store data that is being used by the current program.

3.3.4 ARITHMETIC AND LOGIC UNIT (ALU)

Carries out arithmetic and logical operations such as add, subtract, multiply, process, etc.

Control unit is required to:

(i) Decode and execute the program instructions; and

(ii) Control and coordinate data movements within the CPU and between the CPU and the other components of the computer system.

3.3.5 SECONDARY STORAGE UNITS

The purpose of this is to:

(i) Maintain a permanent store of data and programs when not being used by the computer;

(ii) Maintain a store for the program and data currently being used if the main memory is not large enough to accommodate the entire program and data;

(iii) Serve as a backup of data held in the main memory; and

(iv) Act as a secondary input/output device when the input is in magnetic form or the output is required in a magnetic form.

3.3.6 OUT UNIT

This unit of the computer hardware:

(i) Accepts information/data from the CPU;

(ii) Converts this information/data into the required output form; and

(iii) Sends it to the user through required output device.

SELF ASSESSMENT EXERCISE

- Itemize three major characteristics of a computer system and write short notes on each.

4.0 CONCLUSION

How far have you gone? The unit has successfully introduced to you the definition and meaning of a computer system. You have also learnt

about the general features of the computer system, the classification of computer system based on the data processed/function, size, purpose and technology.

5.0 SUMMARY

A computer can be defined as an electronic device used in processing data and information. It can manipulate and store data for the user's retrieval. Computers have the features –speed, accuracy, reliability, versatility, mass storage capability, precision and security. The classification of computers is based on the size, purpose, data processed/functions and technology.

The hybrid computers process both analog and digital data.

6.0 TUTOR MARKED ASSIGNMENT

With the aid of diagram, show the general layout of a digital computer (The CPU).

ANSWERS TO SELF ASSESSMENT EXERCISE

A computer system has the following three features:

- Speed
- Accuracy and
- Reliability

- **Speed**: Computers are electronic devices and as such, can operate at a fast speed. That makes the computer so fast in operation that in a matter of seconds. It can accomplish what will take human beings days to accomplish.
- Accuracy:
- Reliability:

7.0 REFERENCE/ FURTHER READING

Andrew Feller and Tom Callermann (2006): Value Chains versus Supply Chain, a Journal Presentation.

Charles Parker (2005): Management Information Systems: Strategy and Action McGraw-Hill Publishing.

Ojajuni Jethro (2009): Computer and Business Information System Bookmart SCMS LTD (Publisher) Lagos, Nigeria.

UNIT TWO: COMPUTER HARDWARE AND SOFTWARE TECHNOLOGY

CONTENTS

1.0 INTRODUCTION

The hardware component of a computer is generally defined as the physical part of the system i.e. the part that can be touched both within and without.

The computer hardware has four main sub-components. These include the input, output unit, central processing unit and the auxiliary storage unit. The input unit is the part of the computer system that enables data and instructions to be passed to the central processing unit for processing. Examples of input devices include; mouse, keyboard, joystick, Modem and scanner.

The output unit retrieves data from the CPU and displays it to a form that is readable to human beings. Common examples of output devices are printer, plotter and monitor.

A program is a sequence of instruction which the computer follows (or obey) to perform a specific task. Software is a general term that refers to all forms of programs. The efficiency of the computer depends on the software. Software can be divided into system software and application software.

2.0 OBJECTIVE OF THE UNIT

After you have completed studying this unit carefully, you should be able to do the following:

- Define and explain what computer hardware is
- Discuss the meaning of a computer software technology
- Draw and label a diagram showing the peripheral devices of a computer system.
- Dilate copiously the computer hardware/software technologies storage mechanism.
- Explain the unit measurement in computing

3.0 MAIN CONTENT

3.1.0 HARDWARE

The hardware of a computer system is made up of a number of physical electronic devices connected together as shown in fig. 1.3. The term device is used to describe any piece of hardware that is connected to the processor such as keyboard, monitor, disk drive, printer, scanner,

modem and so on. Such devices are sometimes described as peripheral devices. They may also be classified as input/output (1/0) devices and storage devices.

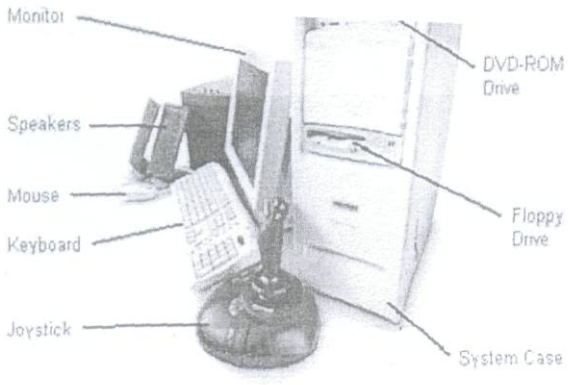
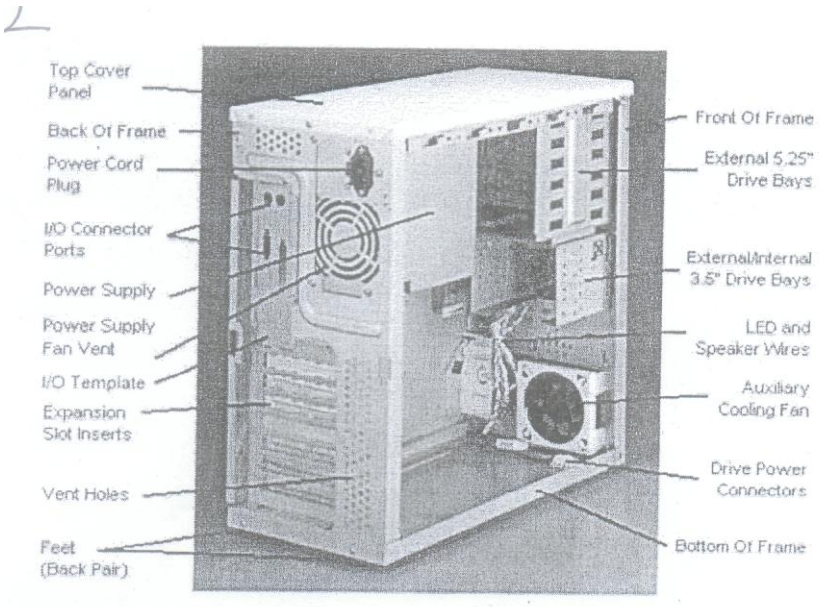


Figure 1.3: The peripheral and internal connections of a computer system.

3.2



A system unit showing the components in a casing

Peripheral Devices

Peripheral is a genetic name for all input/output components and secondary storage devices that depend on direct connection or telecommunication links to the CPU of a computer system. Thus all peripheral devices are on-lone devices, that is, separate from, but can electronically be connected to and controlled by the computer system unit.

1/0 Devices

As the name suggests, 1/0 devices are responsible for communicating with the computer, providing input for the computer to process and arranging to display output for users. The keyboard and mouse are the commonly used input devices. A monitor is the commonest output device that produces a soft copy while a printer device is for hardcopy (paper) output. Storage devices are used to store information in a computer system. The memory unit, Random Access Memory (RAM) is used to store information inside the computer while the computer is switched on. Disks storage is the commonest form of external storage, followed by tapes, floppy disks, Universal Serial Bus (USB) devices.

3.3 COMPUTER HARDWARE/SOFTWARE TECHNOLOGIES

Storage Mechanism

There are several storage devices which may be categorized on the basis of storage and access time, capacity and technology. Another way of classifying storage is by hierarchy. By hierarchy, it refers to the memory that could be used first by the central processing unit (CPU). This classification is done on the basis of the speed of the processing of the memory device.

The speed of the CPU is much faster than the speed of the main and secondary storage. It may be observed that secondary memory are the slowest, main memory is faster than the secondary memory and the cache is faster. The storage capacity of secondary storage devices are the maximum and are usually used for data and programs that are not for immediate use. The main memory storage is bigger than the cache and in terms of cost, the reverse is the case.

3.4 COMPUTER HARDWARE/SOFTWARE TECHNOLOGIES

Everything in the technology environment is either hardware or software. Hardware refers to the physical devices while software are set

of logical instructions that the hardware executes to carry out a particular task.

The **hardware** usually, is used to support the information processing tasks of the computer system. In an information processing system, data/information must be captured using input devices.

Mouse – a device used to highlight, keyboard is the device used to enter the data into the computer.

Pointing devices are used to directly get the data into the computer system, from the source. Example of such are scanners, bar code reader, magnetic ink character recognition etc. conveyed information by presenting it in a form required for use, employing devices like the monitor which allows the soft copy to be displayed printer allows the hard copy to be produced on paper.

3.5 UNITS OF MEASUREMENT IN COMPUTING

Table 1 summarizes the units of measurement used in the describing the world of computers. The processing speed of a computer is enormous compared with the speed at which humans operate. When dealing with units of time, the familiar units of seconds, minutes, hours

and so on, are much too large for describing the time it takes a computer to carry out some of it basic actions. We are sub multiples of a second such as millisecond (1/1000 or 10^{-3}), microsecond 91/1000,000 or 10^{-6}), nanosecond (1/1000 million or 10^{-9}), and picoseconds (1/million millions or 10^{-12}), when measuring the time it takes the processor to carry out its tasks.

Computers are also capable of storing huge amounts of information. The fundamental unit of storage is the byte (also called character). Since this is a small amount of information, bytes are grouped into larger units so that we can easily refer to thousands, millions or billions of them. When counting bytes we deal in powers of 2 such as 2^{10} which is called a kilobyte (Kb), 2^{20} called a megabyte (Mb), 2^{30} called a gigabyte (Gb), 2^{40} called terabyte (Tb). A crucial component of a computer system is a clock, the frequency of which is important in determining a computer's processing speed. Frequency is measured in units called Hertz (Hz) where 1Hz equals one cycle per second and one million Hertz is one megahertz (MHz). This unit is very small when we consider that modern computers operate with clock frequencies of up to 3.5 GigaHertz (i.e. 3500 megaHertz). A basic PC typically operates from 2.5GHz upwards.

TABLE 1: UNITS OF MEASUREMENTS

Storage	Unit Byte	2^{10} Kilobyte (Kb)	2^{30} Megabyte (Mb)	2^{30} Gigabyte (Gb)	2^{40} Terabyte (Tb).
Transmission speed	Bits Per Second	Kilo: Kbps	Mega: Mbps	Giga: Gbps	Tera:Tbps
Time	Unit Second	10^{-3} Millisecond (Ms)	10^{-6} Microsecond	10^{-6} Nanosecond (Us)	10^{-12} Picosecond (Ps)
Frequency	Unit Hertz	10^{3} Kilo Hertz	10^{6} Megahertz	10^{9} Giga Hertz	10^{12} Terahertz

The memory unit is used to store the information (programs and data) that the computer is currently using. It is sometimes called main or

primary memory. One form of memory is called RAM, random access memory. This means that any location in the memory may be accessed in the same amount of time as any other location. Memory access means one of the two things, either the CPU is reading from the memory location or the CPU is writing to a memory location. When the CPU reads from a memory location, the contents of the memory location are copied to a CPU register. When the CPU writes to a memory location, the CPU copies the content of a CPU register to the memory location, overwriting the previous contents of the location.

SELF ASSESSMENT EXERCISE

- Distinguish between a program and operating system

4.0 CONCLUSION

This unit has broadened our mind further so long as CIT 301 is concern. You are beginning to have a clear picture of what information technology 1 is all about. In this unit, you learnt about the definition and meaning of computer Hardware and Software technologies. You have also learnt about the categorization of the computer software technology and the units of measurement in computing.

5.0 SUMMARY

The hardware of a computer system is made up of a number of physical electronic devices connected together.

Peripheral devices are devices outside the central processing unit (CPU) of a computer but which function under the control of the CPU. They include –input, output and Auxiliary storage devices.

A utilities is a program that fills some very specified need, outside the services provided by the operating system.

6.0 TUTOR MARKED ASSIGNMENT

- Discuss succinctly the computer Hardware/Software technologies storage mechanism

Answer to Self Assessment Exercise

A program is a sequence of instruction, which the computer follows (or obeys) to perform a specified task while operating system is a set of programs that controls computer hardware and managers the use of programs.

7.0 REFERENCE/FURTHER READING

Dan Farmer and Wiester Venema (2002): "Forensic Computer Analysis, an Introduction, "Techweb".

Rebecca T. Mercum (2005): Challenges in Forensic Computing, "Communications of the ACM Vol. 48. No. 12."

Olayanju Taiwo (2005): Basic Computer for Schools and Colleges. Daban Printers, Lagos.

UNIT THREE: HISTORICAL LANDMARKS OF COMPUTERS AND E-COMMERCE

CONTENTS

7.0 Reference/Further Reading

1.0 INTRODUCTION

The history of computer development is often referred to in reference to the different generations of computing devices. Each generation of computer is characterized by a major technological development that fundamentally changed the way computers operate, resulting in increasingly smaller, cheaper, more powerful and more efficient and reliable devices.

In 1946 John Neurmann with his associates Arthur W. Burks and Herman H. Goldstine jointly published a paper title “The Preliminary discussion of the logical design of an electronic computing instrument” The paper provided a blue-print for the Von Neumann Machine on which principle the present day computer was built.

Between 1945 and 1950, EDVAC (Electronic Discrete Variable computer) was designed. The machine emphasized the idea of stored program. 1948 Completed prototyped machines at Manchester. Later, Companies like IBM, Remington Corporation. ICL and many others joined in producing computers in commercial qualities.

Therefore the generation of computers are succinctly discussed in his unit, Enjoy it. The unit also examines comprehensively the concept of e-commerce.

2.0 OBJECTIVES OF THE UNIT

Upon successful completion of this unit, you should be able to:

- Discuss the first generation of computers
- Examine the second generation of computers
- Explain the third generation of computers
- Dilate copiously the fourth generation of computers
- Identify the make-ups of the fifth generation of computers.
- Trade the evolution of e-commerce.
- Highlight and discuss the characteristics of e-commerce technologies.
- Explain the potential Risk of e-commerce

3.0 MAIN CONTENT

3.1.0 HISTORICAL LANDMARKS

The history of computer development is often referred to in reference to the different generations of computing devices. Each generation of computer is characterized by a major technological development that fundamentally changed the way computers operate, resulting in increasing smaller, cheaper, more powerful and more efficient and reliable devices.

3.1.1 FIRST GENERATION OF COMPUTERS

These type of computers used vacuum tubes for circuitry and magnetic drums for memory and were often enormous, taking up entire rooms – space almost as large as a lawn tennis court. They were very expensive to operate in addition to using a great deal of electricity, generated a lot of heat, which was often the cause of malfunctions. They relied on machine language, the lowest-level programming language understood by computers, to perform their operations, and they could only solve one problem at a time. Input was based on punched cards and paper tape and output was displayed on printouts. Examples of such generation of computers are the UNIVAC and ENIAC computers.

3.1.2 SECOND GENERATION OF COMPUTERS

Transistors replaced vacuum tubes and that brought in the second generation of computers. The transistor was far superior to the vacuum tube, because it allows this type of computers to become smaller, faster, cheaper, more energy efficient and more reliable than their first generation predecessors. Though the transistor still generated a great deal of heat that subjected the computer to damage, it was a vast improvement over the vacuum tube. Second generation computers still relied on punched cards for input and printouts for output. This with an operating system, which allowed the device to run many different applications at a time with a central program that monitored the memory

Generation of computers moved from binary machine language, to symbolic or assembly languages, which allowed programmers to specify instructions in words. High level programming languages were also being developed at this time. Such as early versions of COBOL or FORTRAN. There were also the first computers that stored their instructions in their memory, which moved from magnetic drum to magnetic core technology.

3.1.3 THIRD GENERATION OF COMPUTERS

The development of integrated circuits (IC) was the hall mark of the third generation of computers. Transistors were miniaturized and placed on silicon chips called semi conductors, which drastically increased the speed and efficiency of computers, instead of punch cards and printouts, users interacted with their generation computers through keyboards and monitors and interfaced with an operating system, which allowed the device to run many different applications at a time with a central program that monitored the memory. Computers for the first time became accessible to a mass of users because of they were smaller and cheaper than their predecessors.

Most computers of this generation were used for both scientific and business data processing applications. Improved software has been designed to provide better control, resulting in efficiency.

3.1.4 THE PRESENT

Fourth Generation Computers

The microprocessor brought the fourth generation of computers, as thousands of integrated circuits were built into a single silicon chip called microchip. A microchip is a flake of silicon, smaller than a finger nail, on which millions of transistors have been etched or built in a

mass production process. Microchip was very much faster, cheaper, reliable and smaller than the previous technologies.

One of the major impacts of the microchip was that it last became feasible to build small and cheap microcomputers. As these small computers became more powerful, they could be linked together to form networks, which eventually led to the development of virtual computing via virtual networks. Fourth generation computers also saw the development of Graphic User Interface (GUI), deploying mouse and hand held devices.

3.1.5 THE FUTURE

Fifth Generation Computers

Fifth generation computing devices, based on artificial intelligence are still in development, though there are some applications such as voice recognition that are being used today. The use of parallel processing and superconductors is helping to make artificial intelligence a reality. The goal of the fifth generation computing is to develop devices that respond to natural languages as input and are capable of learning and self-organizing. That is, computers of this generation should be able to perform the following tasks with little or no human intervention:

(a) Problem-solving and inference

(b) Knowledge based management; and

(c) Intelligent interface with the user.

Each type of computing machine would be capable of simulating a limited narrow range of human behaviour. For example, computers could be able to diagnose illnesses and recommend treatment (personal doctor system); machines that diagnose faults to computers and initiate repairs (personal maintenance system); machines that provide legal advice (personal lawyer system); machines that provide financial advice (personal financial system); machine that run factories. These are examples of machines that perform many (not all) actions normally associated with physicians, auto mechanics, lawyers, accountants and assembly line workers, respectively. They are collectively referred to as expert systems. These are systems that would ordinarily carryout normal tasks that should be performed by humans.

3.2.0 EVOLUTION OF E-COMMERCE

A computer network is a collection of computers and devices connected to each other. The network allows computers to communicate with each other and share resources and information. There are different types of computer network depending on the number of computers and devices that make the network.

A type of computer network is the internet. The internet is a specific inter-network of computers. It consists of a worldwide interconnection of governmental, academic, public and private networks. It enables users to share information along multiple channels. Typically, a computer that connects to the internet can access information from a vast array of available computers on the internet by moving information from them to the computer's local memory. The same connection allows that computer to send information to the computers on the network; that information is in turn accessed and potentially modified by a variety of other interconnected computers.

The rapid growth of the internet led to the search for improved techniques for conducting effective business and commercial activities on the internet. E-commerce in a broader sense, started much earlier, when telephones and fax machines were used to place orders for buying

product or services. For example, an interactive voice recording system is a system that plays an appropriate recorded voice on the telephone line when a customer presses some predefined digits on the telephone.

Thus the major requirements to establish E-commerce activity are the creation of information base, processing capabilities of information and an effective mechanism for information communication within and outside the organization.

3.2.1 CHARACTERISTICS OF E-COMMERCE TECHNOLOGIES

The characteristics of e-commerce technologies include:

(a) Ease of automated processing

A payer can cheaply and easily automate the generation and processing of multiple payments with minimal effort. Previously, the dependence upon banks to handle most payments and the lack of a cheap, ubiquitous communications technology made automation of payment processes expensive and difficult to establish.

(b) Instant result

Payment is immediate because automation and the ability for the intermediate system and providers to process payments in real-time. With manual and paper-based systems there is always a time delay due to the requirement for human intervention in the process.

(c) Openness and accessibility

The availability of cheap computing and communications technology and the appropriate software enables small enterprises and individuals to access or provide a range of payment services that were previously only available to large organizations via dedicated networks or the transactional processing units of banks.

(d) Loss of collateral information

The new technology dispenses with, or alters, collateral information accompanying transactions. This information has traditionally been part of the transaction, and has been relied upon by the transacting parties to validate individual payments.

Collateral information can be defined as information:

(i) Which is not essential to the meaning and intent of a transaction; and

(ii) Which is typically incidental to the nature of the communications channel over which the transaction is conducted; but nevertheless provides useful contextual information for one or more of the parties to the transaction.

Collateral information can include many things ranging from tone of voice in a telephone call to the business cards and letterheads and apparent authority of the person with whom you are dealing.

Now that information is received not only via a single channel (such as an electronic message) new processes need to be put in place to support and reinforce payments in the same way as manual systems.

(e) Globalization

Globalization, or the removal of distance barriers in making payments, has been an obvious aspect of the new payments systems. Its effect is upon areas such as size of the payments marketplace, uncertainty as to legal jurisdiction in the event of

disputes, location and availability of transaction trails, and the ability of a payment scheme to rapidly adapt to regulatory regimes imposed by one country when moving funds to another.

(f) New Business Models

New business models are being developed to exploit the new payment technologies, in particular to address or take advantage of the disintermediation of customers from traditional payment providers such as banks. In this context, disintermediation is where the technology enables a third party to intervene between the customer and the banking system, effectively transferring the customer's trusted relationship with the bank to the new party.

3.3 POTENTIAL RISK OF E-COMMERCE

3.3.1. SIMULATED ONLINE APPROVAL ATTACK

Internet payments are susceptible to attack due to the accessibility and openness of the Web. In this attack, the perpetrator compromises the merchant's Web link to their online payments gateway. Once compromised, any request for payments approval will always be positive regardless of whether funds are available or not, and initiates

authorization from the bank, which in turn would initiate delivery of the goods or services by the merchant. It would only be much later that reconciliation of the bank accounts with the online merchant facility detected any discrepancy. Purchase of goods using false credit cards/debit cards becomes feasible once the merchant link to the bank has been compromised.

3.3.2 REMOTE PIN CAPTURE ATTACK

As traditional payments channels have become Web enabled, sophisticated techniques to capture logon IDs and PINs have evolved based upon using installation of PIN capture software on the users PC. An example of such software are the DIRT (Data Interception by Remote Transmission) [1], Sub Seven and B02K Trojans. They enable remote logging of keystrokes and capture of payments details and are installed via activation, email attachments or logging onto an infected Web site. This information is automatically emailed or transmitted to the attacking party, enabling exploitation of the various services.

SELF ASSESSMENT EXERCISE

- Globalization is a senequanon to the general characteristics of e-commerce technologies. Discuss

4.0 CONCLUSION

Unit three of module 1 of information technology 1 is interesting in the sense that the historical Land Mark which is in reference, the various generations of computers took time to explain the developmental stages of the computers we are using today-first Generation, Second Generation, third Generation, Fourth Generation and Fifth generation each accompanying notable features and concrete examples. You have also learnt about the evolution of e-commerce, characteristics and its potential risks.

5.0 SUMMARY

The historical landmarks of computers span from the first generation, second generation, third generation, fourth generation to the future generation otherwise known as the fifth generation of computers. The characteristics of e-commerce technologies include

- Ease of automated processing, instant result, openness and accessibility etc.

6.0 TUTOR MARKED ASSIGNMENT

- Explain clearly with good examples the future generation of computers.

ANSWERS TO SELF ASSESSMENT EXERCISE

Globalization: Is one of the major characteristics of e-commerce. Globalization, or the removal of distance barriers in making payments, has been an obvious aspect of the new payments system. Its effect is upon areas such as size of the payments, market place uncertainty as to legal jurisdiction in three event of location and availability of transaction trails, and the ability of a payment scheme to rapidly adapt to regulatory regimes imposed by one country when moving funds to another.

7.0 REFERENCE/FURTHER READING

Olayanju Taiwo (2005): Basic Computer studies for schools and colleges. Daban Printers Ltd. Lagos, Nigeria.

Ojajuni Jethro (2009): Computer and Business Information System. Bookmart SCMS Publishers Ltd, Lagos, Nigeria.

Thursday Bram (2003): "What is Grid Computing Conjecture Corporation.

UNIT FOUR: THE COMPUTER INPUT AND OUTPUT DEVICES

CONTENT

1.0 INTRODUCTION

The computer input is made up of all the input devices such as keyboard, mouse, monitor, optical mark recognition, optical character recognition, terminal, typewriters, etc.

An input device is a medium by which data can be transferred to the computer memory. Probably the most common way, in which you will input data, at least at the beginning, is by using a keyboard. These devices convert numbers, letters and special characters that people understand into electrical signals. These signals are sent to and processed by the system unit. The input devices act as an interface by accepting the data in human readable form and presenting it to computer in its own recognizable form.

The output devices are used to transmit processed data to the users. These are visual display units (VDU), printers, etc. Since communication has to be two-way, the computer also needs to employ a device to communicate with the user. The result of computer work is output.

The secondary storage devices hold data, even when computer is turned off.

2.0 OBJECTIVES OF THE UNIT

At the end of this unit, you are expected to:

- Differentiate between the input and output devices
- List and explain the usefulness of some of the input and output devices.
- Discuss the major output devices with examples.
- Highlight the speech input devices and explain item.
- Explain the usefulness of a magnetic tape, graph plotter, dot matrix, plotters Daisy wheel etc.
- Discuss the usefulness of a floppy diskette and modem.

SELF ASSESSMENT EXERCISE

- Critically distinguish between magnetic diskettes and magnetic tape unit if any.

3.1.0 INPUT/OUTPUT DEVICES

The computer will be of no use unless it is able to communicate with users. Input/output devices are required for users to communicate with the computer. Input devices bring data/information into the computer and output devices are used to bring out the information from the system. Input/output devices are also known as peripherals. The input

device encodes data/information into machine readable form. The output device on the other hand decodes the information in a readable form into one that is understood by the computer user. Some of the commonly used input/output devices are listed in Table 1.2

Input Devices	Output Devices
Keyboard	Monitor
Mouse	LCD
Joystick	Printer
Light pen	
Scanner	
Optical character reader	
Bar code reader	

Table 1.2 input and output devices

3.1.1 THE KEYBOARD AS INPUT DEVICES

This is a text-based input device that allows the user to input alphabets, numbers and other characters. It consists of a set of keys mounted on a board. Such keys include:

(i) Function keys labeled F1, F2……F12, Functions assigned to these keys differ from one software package to another. These keys are also user programmable.

(ii) Alphanumeric keypad. It consists of keys for English alphabets, 0 to 9 number and special characters like +, - /*etc. Some keys also contain alphabets of other languages.

(iii) Other special keys like ENTER, Space bar, Back space, Delete, Insert, Shift, Caps Lock, Tab, Ctrl, Alt, Esc, Numeric Key pad and Cursor movement keys.

The keyboard is one of the most popular input devices. A typical keyboard is shown in the diagram below.

Figure 1.5 Keyboard

3.1.2 POINTING DEVICES

These devices allow users to issue commands or make choices by moving a cursor on the display screen. Pointing devices allow the user to easily choose from menu selections and icon display using point-and-click-and–drag method. The point and click/drag and drop operations are enabled by the Graphic User Interface technology)GUI).

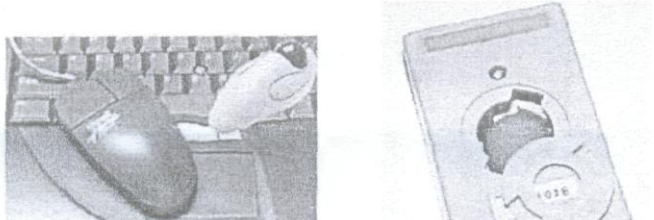
Icons are small objects that look like familiar devices such as folder, calculator, waste basket etc. Using icons help simplify computer use, as they are easier to use with pointing devices than menu and other text-based displays. Examples of pointing devices include:

(i) **Mouse:** This is a small device used to point to a particular icon on the screen and select in order to perform one or more actions. It can be used to select menu commands, resize winders, start program etc.

The most conventional kind of mouse has two buttons on top: the left one being used most frequently.

The figure 1.6 shows two typical mice

The figure 1.6 shows two typical mice



Most actions being performed by a mouse include:

- Left click – Used to select an item
- Double click – Used to start a program or a file
- Right Click-Usually used to display a drop-down window of commands.
- Drag and drop – Allows one to select and move an item from one location to another on the input screen.

(ii) **Joystick**: This is a vertical stick which moves the graphic cursor in a direction the stick is moved. It typically has a button on top that is used to select the option pointed by the cursor. Joystick is primarily used as an input device with video games, and controlling robots.

(iii) **Track Ball**: While a mouse employs a rolling ball on its underside, a trackball uses an exposed ball that the user manipulate with the fingers. Like the mouse, it is used to move the cursor on the display screen. It does not require a horizontal pad on which to move.

(iv) **Touch Screen**: This allows the user to operate or make selections by simply touching the display screen. Modern hand-held computers (PDA) use touch screen.

(v) **Light Pen:** This is a pen-shaped device used to select objects on the display screen. It is like the mouse in the way if functions. However, it uses a light pen to move the pointer and select any object on the screen by pointing to the object.

3.1.3 OPTICAL SCANNING DEVICES

These are devices that read text or graphics and convert them into digital input to the computer system for further processing. It enables direct entry of data from the source document (document, picture, etc) where it is eventually converted into a digital form.

Some of the other scanning technology devices explained are:

(i) Magnetic Ink Character Reader (MICR)

This is a method of data entry widely used in the banking system to process cheques. Each cheque has an identifying information (cheque number, account code, and banks sort code), printed in magnetic ink.

(ii) Optical character reader

Optical character recognition OCR, though, different from magnetic ink character recognition, is similar in concept. Whereas the OCR optically detects the characters on the document and converts them to codes which are then sent to the processor, the MICR magnetically detects the characters. The OCR reads characters and codes on items like merchandise tags, product labels, credit card receipts, utility bills, airtime tickets and other documents like marked multiple-choice examination sheets, OCR can handle almost any font.

(iii) Scanner

This is an input device used for direct data entry from the source document into the computer system. This converts the document,

picture images into digital form so that they can be fed into the computer. Capturing information like this reduces the possibility of errors typically experienced during large data entry. Hand held scanners are commonly seen in retail stores and supermarkets to scan codes and price information for each of the items.

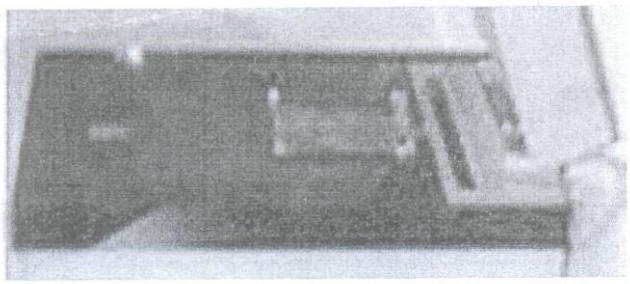


Figure 1.8 Scanner

(iv) Bar Code Reader

This is a special type of scanner that is used to input data from bar codes. A bar code is a set of lines of different thickness that represent different numbers. Most products in retail shops or supermarkets have bar codes on them.

A bar code reader operates by shining a beam of light on the lines that make up the barcode and detecting the amount of light that is reflected back.

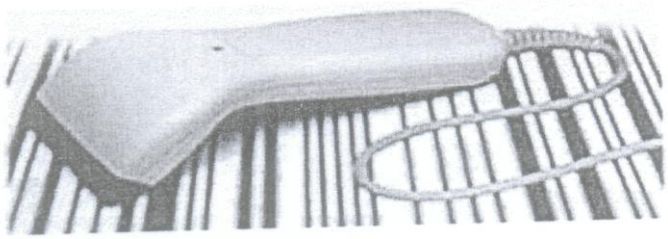


Figure 1.9 The Bar Code Reader

(v) Magnetic strip technology

This is technology that reads information on magnetic strip on a plastic card. Such devices include:

- Transaction terminals

  These capture data from users during transaction and transmit it over telecommunication networks to a computer system for processing. Examples are the banks Automated Teller Machine (ATM), credit card, debit card, point –of-sale POS etc.

3.2 OTHER INPUT DEVICES

Other types of input devices that may be used by the computer system include sound input device (microphone), and biometric device (for capturing biodata).

3.2.1 DIGITAL CAMERA

A digital camera can store many more pictures than an ordinary camera. Pictures taken using a digital camera are stored inside its memory and can be transferred to a computer by connecting the camera to it. A digital camera takes pictures by converting the light passing through the lens at the front into a digital image.

Figure 1.10 Digital Camera

3.2.2 THE SPEECH INPUT DEVICE

A speech –input device allows the use of microphone as an input device. A speech-recognition program then processes the input and corrects it into machine-recognized commands or input. A sound card installed on the computer digitizes audio input into 0 and 1's. Example is the microphone–speech recognition device show-below:

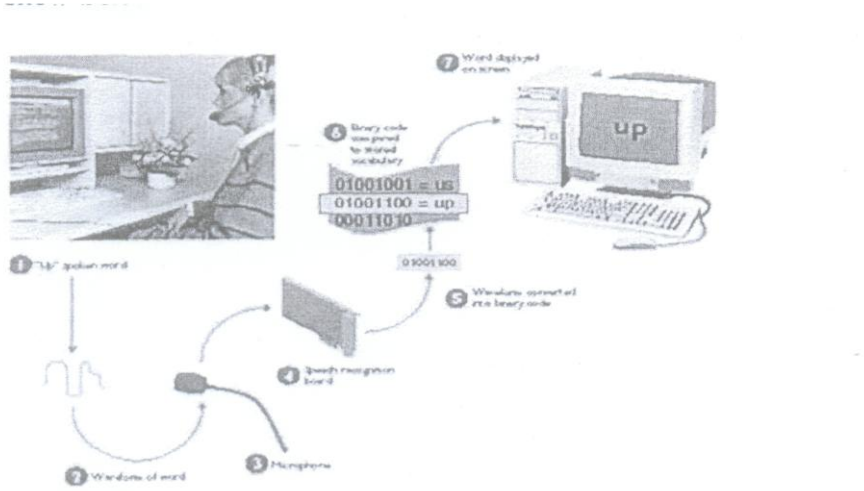


Figure 1.11 The Microphone - Speech Recognition Device

3.3 OUTPUT DEVICES

Monitor

These are the commonest output devices for a computer system and they produce a soft copy of the document requested. A soft copy is an output that does not persist over time. Monitors are of different types.

3.3.1 VISUAL DISPLAY UNIT (VDU)

This consists of a cathode ray tube (CRT) to display output together with the keyboard to accept input. The combination allows a dialogue with the computer. The application of a VDU is limited to those where no permanent record of output is required. A VDU is shown in figure 1.12.

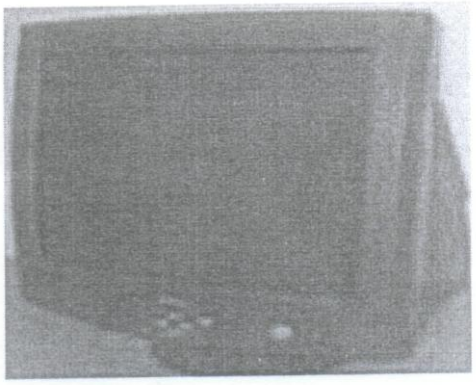


Figure 1.12 A Visual Display Unit

3.3.2 LIQUID CRYSTAL DISPLAY (LCD)

This is a display technology that uses liquid crystal solution. Also, called 'flat screen', they are slow and sleek, when compared to CRT monitors and power consumption is minimal.

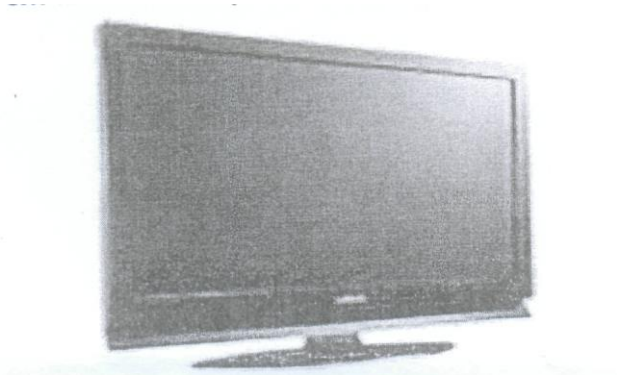


Figure 1.13 A Liquid Crystal Display

3.4 PRINT OUTPUT DEVICES

After video displays, document print output is the most common form of visual output for the user. Print output is being produced in a hardcopy form. A hardcopy output such as printed paper or microfilm is one that persists over time. Print output is important for permanent records at least in hardcopy form. It is portable and may be posted or delivered to

end users. There are different types of printers all offering different mix of:

(a) Speed;

(b) Quality of output

(c) Range of print fonts

(d) Graphics capabilities

(e) Cost of purchase

(f) Cost of operation; and

(g) Associated noise level.

Based on technology used, printers may be classified as impact or non-impact printers.

Impact printers are those that use the typewriter printing mechanism wherein a hammer strike the paper through a ribbon in order to produce output. Don't matrix and character printers fall under this category.

3.4.1 DOT MATRIX PRINTER

This type of printer has a movable print head, which consists of a matrix of pins. The set of pins corresponding to the shape of the

character to be printed is impacted on the ribbon which then leaves an inked image on the page. A dot matrix printer is shown in figure 1.14.

Dot mat printers are commonly used in retail stores and banks to print documents and receipts. Some ATM machines are equipped with dot matrix printers. Dot matrix is also used in industries. Dot matrix printers have some advantages for their use. Printing is not hampered when the ribbon is low in ink, although printing quality may be faded. Dot matrix printers are durable, because they do not contain highly sensitive components like other modern day printers. One disadvantage of these printers is that they can be quite noisy and could be rather annoying to use.

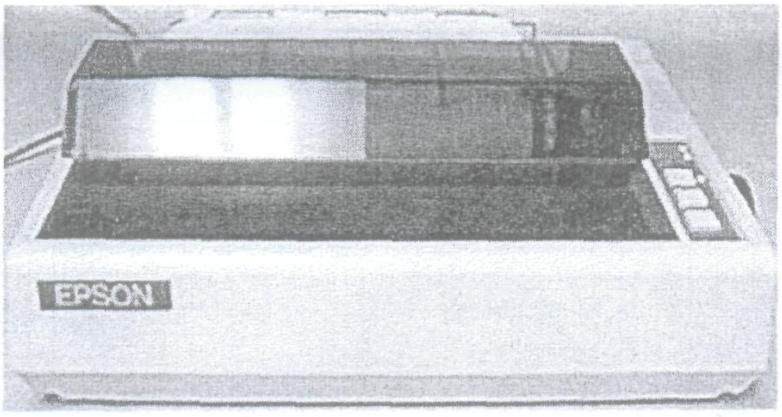
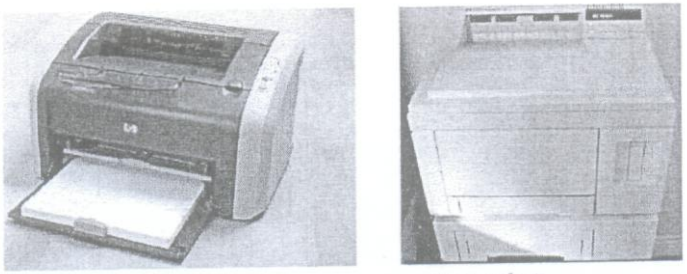


Figure 1.14 An EPSON Dot Matrix Printer

3.4.2 INKJET PRINTERS

This type of printers ejects a stream of special ink through a fine nozzle to form the characters that are painted on the paper. Inkjet printers provide good output quality. They can also provide a variety of fonts and pronounce diagrams. Modern inkjet printers can also produce high-quality multi-coloured output. They are quite in operation. Figure 1.15 depicts and deskjet printer.



Deskjet Laserjet

Figure 1.15 HP Deskjet and Laserjet printers

(ii) Laserjet

This is a popular printer generally used in making large volume printing especially Desktop Publishing (DTP). Its operation is very similar to that of the photocopying machines. The laser beams are sued to create

an image of the document on a drum coated with photoelectric material. When the paper comes in contact with the drum, a permanent image is printed on paper with the help of the toner. Speed of the laserjet printer is measured as dots per inch (dpi).

3.4 PHYSICAL STORAGE DEVICES

3.4.1 Data Representation

Computers work with some specific number of bits. Common collections are single bits groups of four bits (called nibbles) groups of eight bits (called bytes) groups of 16 bits (called words) and more. The sizes are not arbitrary.

Bits

The smallest "unit" of data on a binary computer is a single bit. Since a single bit is capable of representing only two different values (typically zero or one) one may get the impression that there is very small number of items you can be represented with a single bit. Not true! There are an infinite number of items you can represent with a single bit.

With a single bit, one can represent any two distinct items. Examples include zero or one, true or false, on or off, male or female and right or

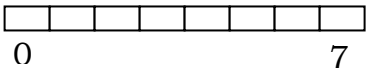
wrong. However one is not limited to representing binary data types (that is those objects which have only two distinct values). You could use a single bit to represent the number 823 and 1245. Or perhaps 625 and 4 and 5. One can also use a single bit to represent the colours red and blue.

Nibble

A nibble is a collection of four bits. It is not a particularly interesting data structure except for two items: BCD (binary coded decimal) numbers and hexadecimal numbers. It takes four bits to represent a single BCD or hexadecimal digit. With a nibble one can represent up to 16 distinct values. In the case of hexadecimal numbers, the bits ("The Hexadecimal Numbering System"). BCD uses ten different digits (0 1 2 3 4 5 6 8 9 A B C D E and F are represented with four bits ("The Hexadecimal Number System"). BCD uses ten different digits (0 1 2 3 4 5 6 8 8 9) and requires with a nibble but hexadecimal and BCD digits are the primary items one can represent with a single nibble.

Byte

A byte consists of eight bits and is the smallest addressable datum (data item0 on the microprocessor. Main memory and 1/0 addresses are all byte addresses. This means that the smallest item that can be individually accessed by a program is an eight-bit value. To access anything smaller requires that you read the byte containing the data and mask out the unwanted bits. The bits in a byte in a byte are normally numbered from zero to seven using the convention shown below:



Bit 0 is the low order bit or least significant bit of the byte. Bit 8 is the high order bit or most significant bit of the byte. Reference to all other bits is by their number and note that a byte contains exactly two bibles.

Bits 0..3 comprise the low order nibble bits 4..8 form the high order nibble. Since a byte contains exactly two nibbles byte values require two hexadecimal digits.

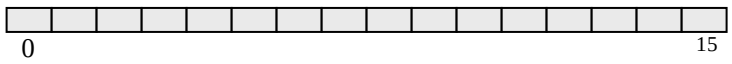
Since a byte contains eight bits it can represent 2^8 or 256 different values. Generally, a byte will represent numeric values in the range

0…255 with signed number in the range -128.. + 128. ASCII/IBM character codes and other special data types requiring no more than 256 different values. Many data types have fewer than 256 items, so eight bits is usually sufficient.

Probably the most important use for a byte is holding a character code. Characters typed at the keyboard displayed on the screen and printed on the printer all have numeric values. To allow it communicate with the rest of the world the IBM PC uses a variant of the ASCII character set (see "The ASCII Character Set"). There are 128 defined codes in the ASCII character set. IBM uses the remaining 128 possible values for extended character codes including European characters graphics symbols, Greek letters and math symbols.

Computer word

A word is a group of 16 bits. We could number the bits in a word starting from zero on up to fifteen. The bit numbering appears below:



Like the byte bit 0 is the low order bit and bit 15 is the high order bit. When referencing the other bits in a word use their bit position number.

Notice that a word contains exactly two bytes. Bits 0 through 8 from the low order byte bits 8 through 15 form the high order byte:

Naturally a word may be further broken down into nibbles as shown below:

Nibble zero is the low order nibble of the word and nibble three is the high order nibble of the word. The other two nibbles are “nibble one” or “nibble two”.

With 16 bits you can represent 2^{16} (65,536) different values. These could be the values in the range 0..65,535 (or as is usually the case – 32 868..+32 868) or any other data type with no more than 65 536 values. The three major uses for words are integer values offsets and segment values.

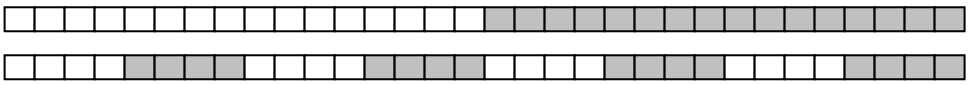
Words can represent integer values in the range 0..65 535 or – 32 868.. 32 868. Unsigned numeric values are represented by the binary value corresponding to the bits in the word. Signed numeric values use the two’s complement form for numeric values (see “Signed and Unsigned Numbers”). Segment values which are always 16 bits long

constitute the paragraph address of a code data extra or stack segment in memory.

Double words

A double word is exactly what its name implies a pair of words. Therefore a double word quantity is 32 bits long as shown below:

Naturally this double word can be divided into a high order word and a low order word or four different bytes or eight different nibbles.



Double words can represent all kinds of different things. First and foremost on the list is a segmented address. Another common item represented with a double word is a 32-bit integer value (which allows unsigned numbers in the range 0..4 294 968 295 or signed numbers in the range -2 148 483 648...2 148 483 648). 32-bit floating point values also fit into a double word. Most of the time, double words are used to hold segmented addresses.

3.6 HARD STORAGE DEVICES

Secondary storage devices hold data, even when computer is turned off. The physical material that actually holds such data is called "storage medium". All computers require permanent storage facilities. This is because the main memory within the CPU is limited in size, and in the even of power failure the contents of this main memory disappear.

The purpose of secondary storage (also known as backup or external storage), is to:

(a) Maintain a permanent storage of data and program when not being used by the CPU.

(b) Maintain a store for the program and data currently being used, if the main memory is not large enough to accommodate the entire program and data.

(c) Maintain a copy of data held in the main memory for security purposes.

(d) Act as a secondary input/output device when the input is in magnetic form or the output is required in magnetic form.

Two primary storage technologies are magnetic and optical.

3.6.1 MAGNETIC STORAGE

The primary types of magnetic storage are Hard disks, diskettes (floppy disks) disk cartridges and magnetic tape. These include:

(a) The Hard Disk

In order to increase the storage capacity of a disk and decrease its access time it is necessary to use a hard disk. Hard disks as shown figure 1.16 are single, hard, magnetic disk(s) sealed within their own drives. This environment is protected from dust. They can rotate at faster speeds than the floppy disks and rather than read/write head being in contact with the surface of the disk, it floats just above it.

The surface of each of the disks (if more than one) is divided into tracks and each tracks is divided into sectors. There may be from forty (40) to hundreds (100) of tracks on a disk surface. Each sector of a track will typically have a capacity from 32 to 1024 (1kb) bytes. Information/data is stored or read from a disk magnetically, using a read/write head. To access information on a disk, the head must be moved to the correct track. The time taken to do this is called seek time'. The correct sector

must rotate around the head. The time taken to do this is referred to as rotational delay or latency and finally, the information may be transferred (transferred time). On a typical Hard disk, the average seek time is less than twenty 20ms (twenty milliseconds). Based on disk rotation speed of 3600, revolution per minute, (rpm), the average rotational delay in the time for half of one rotation, about 8ms.

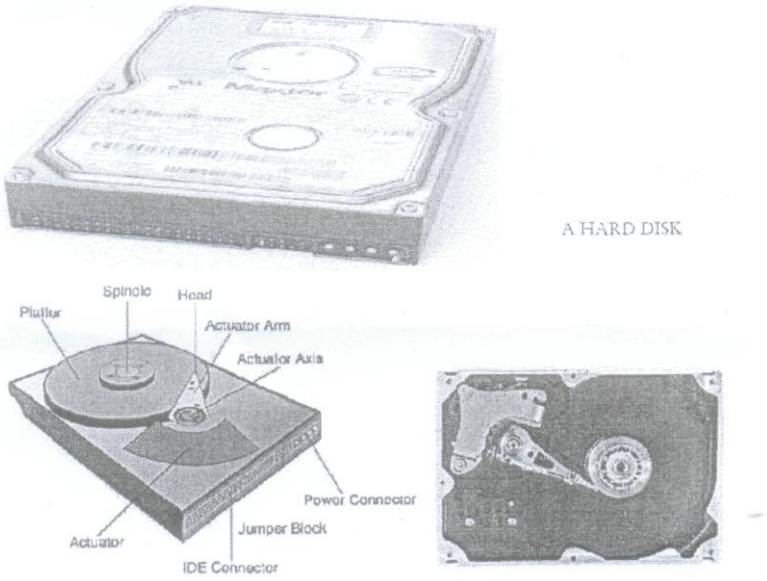


Figure 1.16: A Hard disk

3.6.2 FLOPPY DISKETTE

The floppy disk is a small sized auxiliary storage device commonly used for storing the data and programs. The floppy disk is inserted into the disk drive before writing or reading data from disk. The floppy disk may be logically though of as a magnetic disk. It is logically divided into several circles called tracks. Each tracks is further partitioned into sectors where data for retrieval or storage are placed. Each sector within each track can occupy 512bytes of data.

The floppy disks is covered with a rigid envelope. For reading and writing on disk, the head has to be in contact with the disk surface which is used to store data and read data stored in the floppy disk. The capacity of a floppy is measured as the maximum storage size. The floppy available today may store as much as 1.44 Megabytes (MB) of data. Figure 1.17 shows a typical floppy diskette

ette.

Figure 1.17: A Floppy diskette

3.6.3 TAPE DISK, COMPACT DISK READ ONLY MEMORY

Tape Storage

Magnetic tape stores data in form of records. Several records are collected together and stored in a block. Between these blocks of data are parts of the tape on which no data in stored. These are called inter block gaps. There is a header label that gives information such as the name of the tape, the name of the program that is used to update it and the last date of update. When reading or writing data, the tape drive passes the tape from reel to reel over a read/write head, which either reads data into the processor or write from CPU to the tape. The tape is a sequential storage medium. This means that to access the nth item of information, the device has to skip over the first (n-1) items.

This makes the tape very slow to access in comparison with magnetic disks. Typically, tape storage is used to keep a backup of the information stored on a disk or information that may not be needed for urgent processing.

Tape is popular in big computers where large amounts of data (mass storage), have to be kept for years.

3.7 OPTICAL STORAGE

The storage efficiency and access speeds for magnetic disk systems are limited to the moving mechanical parts, and by the density with which data can be packed on the storage medium.

Optical disk technology consists of encoding data as a series of microscopic pits on the surface of a disk that is covered with a transparent plastic coating. These pits can be read by means of laser light focused with great accuracy onto the spinning disks. An optical storage disk is shown in figure 1.18

(a) CD-ROM (Compact Disk Read-Only Memory): This is WORM (Write Once, Read Many Times) device that is capable of read only access but very much large storage. Optical scanning techniques,

using lasers, are employed with CD-ROMs which allow massive amounts of data to be stored in a compact area. CD-ROM is more reliable and durable than magnetic media (disks and tapes). In terms of capacity, a single CD-ROM may store up to 800 megabytes. In terms of text, this is equivalent to about 200 books of 1000 pages each.

(b) CD-R: CD recordable is a storage medium that combines the reliability and storage capacity of CD-ROM with the flexibility of magnetic disks because it allows users to store their information on them. However, a CD-R does not allow the recorded data on it to be erased.

(c) CD-RW: CD rewritable optical disk system also functions like the CD-R, but it can be written and overwritten repeatedly, just like a hard disk.

(d) DVD – (Digital Video Disk or Digital Versatile Disk) whose capacity ranges from 4.8GB upwards are now replacing the CD-ROMS. A special drive is needed to read these DVD disks and write to them. DVD disks are commonly used for distributing films as a rival to video tapes. DVD rewritable (DVD-RW) is also available.

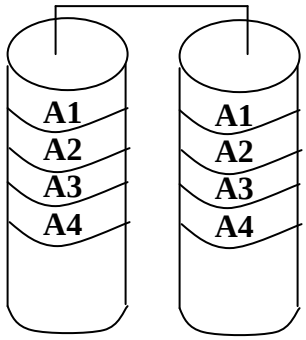
3.7.1 REDUNDANT ARRAYS OF INEXPENSIVE DISKS (RAID0 TECHNOLOGY

The physical size of hard disks has decreased dramatically over the years. Some years ago, a hard disk of say 100MB capacity was considered larger. These days, such a multi-gigabyte disk fits easily inside a laptop computer. The cost also has fallen in a similar manner. The shrinking size and low cost of disks has led to the use of systems with several disks, the Redundant Arrays of Independent Disks.

In a RAID system, information is distributed over a number of disks in such a fashion that if one of the disks is removed from the system (due to failure), the information can still be accessed. Basically RAID is when two or more hard disks are combined in a way to either increase performance, add data protection (fault tolerance) or both. It is a very useful technology for today's high demand storage subsystems with practical and affordable configurations from home-desktop systems to high-end workstations or severs. Figure 1.19 shows a simple version of RAID system mirroring whereby two disks whose contents are mirror images of each other are maintained. Whenever information is stored (updated) on one disk it is automatically stored (updated) on its mirror

disk. In the event of one of the disks failing, then the second can be sued to access the information. In this case we have 100% redundancy that is, a complete copy of information is stored on the second drive.

RAID 1



Disk 0 Disk 1
Figure 1.19: A RAID 1 SYSTEM

This increases the availability of data in the system at the expense of a second disk. Using clever software however, similar availability can be achieved in a system without the overhead 100% redundancy. A RAID system might be composed of nine (9) disks where eight (8) of the disks are used to store information and one (1) disk is used to store redundant information. This redundant information can be used to reconstruct data from any of the disks in the event of a disk failing. With this arrangement, there will be a little percentage of redundancy, but the system can operate successfully without information loss, if any of the disks becomes faulty.

4.0 CONCLUSION

In this unit, you have learnt about the various input and output devices. Digitizer, card reader, Bar code reader, touch screen, magnetic ink character recognition (MICR) are all input devices. Computer output devices as you have learnt in this unit comprise – printer, monitor or VDU, graph plotter, magnetic tape etc.

5.0 SUMMARY

The computer will be of no use unless it is able to communicate with users. Input/output devices are required for users to communicate with the computer. Input devices bring data/information into the computer and output devices are used to bring out the information from the system. Input/output devices are also known as peripherals. The input device encodes data/information into machine readable form.

7.0 TUTOR MARKED ASSIGNMENT

- Write short note on the following

(i) Joystick (ii) Track Ball (iii) Touch screen (iv) Light Pen.

ANSWER TO SELF ASSESSMENT EXERCISE

Magnetic Disc Reader has a dual purpose capacity of input and output for reading and recording respectively.

Each disk is inserted into a narrow slot in the front of the disk drive. While magnetic tape unit reader also has a dual purpose capacity of input and output for reading recording. It holds the magnetic tape reel and also a second reel for taking up tape. Similar in concept of a tape recorder.

7.0 REFERENCE/FURTHER READING

A. I. Ibrahim (2006): Introduction to Computer; Alderson Publishers, Ogun State, Nigeria

SQL Serve (2008): Books Online Data Integrity Thera Radhakaishnan, "E-governance".

Thursday Bram (2003): "What is Grid Computing Conjecture Corporation.

Yadav D.S. (2000): "Koundations of Information Technology, New Age International Publishers.

MODULE TWO

UNIT ONE: THE COMPUTER NET WORK AND CABLING

UNIT TWO: COMPUTER NETWORK TOPOLOGY AND GENERAL E-COMMERCE

UNIT THREE: COMMUNICATIONS SUPPORTED BY INFORMATION TECHNOLOGY

UNIT FOUR: ELECTRONIC FILES TRANSFER/SECURITY

UNIT ONE

THE COMPUTER NET WORK AND CABLING

CONTENT

1.0 INTRODUCTION

A network can be defined as the interconnectivity between an independent computers and a semi independent computers in other to share resources such as printer, data base and file etc. It can be defined as the interconnection of computers or computer devices such as (Printer, data and storage system) via some form of communication facility such as public telephone, radio, satellite or private lines to exchange information.

Independent computer can print, store and process data alone. A semi independent computer is a computer that has two features (input or output) computer network can be grouped into:

- LAN – Local Area Network
- MAN – Metropolitan Area Network
- WAN – Wide Area Network

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with networks. In some case, a network will

utilize only type of cable, other networks will use a variety of cable types.

2.0 OBJECTIVES OF THE UNIT

After you mighty have finished reading this unit, you should be able to:

- Define and explain what a computer network is
- Itemize the relative advantage of computer network.
- Examine the disadvantage of network.
- Explain the computer network cabling.
- Enumerate and explain types of computer networks.
- Examine the wide area network and discussing the wireless local area networks.

3.1.0 NETWORK COMPONENTS, CONFIGURATION AND DESIGN

Introduction

Computer network consists of two or more computers that are linked in order to share resources such as printers and CD-ROMs, exchange files, or allow electronic communications. It may also be defined as a

collection of resources among themselves. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

3.1.2 ADVANTAGES OF COMPUTER NETWORK

(a) Speed: Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks or any other storage medium, then copying the files to one or more computers. This method of transferring files is very time-consuming.

(b) Cost: Integrated software that may be used on a network are now available at considerable savings as compared to buying individually licensed copies. Besides monetary savings, sharing a program on a network allows for easier use of program by multiple users simultaneously.

(c) Security: Files and programs on a network can be well secured. Also, passwords can be established for specific directories to restrict access to authorized users.

(d) Centralized software management: One of the greatest benefits of installing a network is the fact that all of the software can be loaded on one computer (the file server). This is eliminates the need to spend time and energy installing updates and tracking files on stand-alone computers throughout the organization.

(e) Resources sharing: Sharing resources is another area in which a network exceeds stand-alone computers. Most organizations cannot afford enough laser printers, fax machines, modems, scanners, and CD-ROM players for each computer. However, if these or similar peripherals are added to a network, they can be shared by many users.

(f) Electronic Mail: The presence of a network provides the hardware necessary to install an e-mail system. E-mail aids personal and professional communications and it facilities the dissemination of information within an organization. In a typical network environment, one computer is designated as the file server. It stores all the software that control the network, as well as the software that can be shared by the computers on the network. Computers connected to the file server are called workstations. The workstations can be of less capacity than the file server, and

they may have additional software on their hard disks. On most networks, cables are used to connect the computers.

(g) Flexible Access: School networks, for example, could allow students to access their files from computers throughout the school. Students can begin an assignment in their classroom. Save part of it to a public access area of the network, and then go the media centre after school to finish their work. Student can also work cooperatively through the network.

(h) Workgroup computing: Workgroup allows many users to work on a document or project concurrently. For example, educators located at various schools within a country could simultaneously contribute their ideas about new curriculum standards to the same document and spreadsheets.

3.1.3 DISADVANTAGES OF COMPUTER NETWORKS

(a) **Expensive to install**: Although a networks will generally save money overtime, the initial costs of installation can be prohibitive. Cables, networks cards, and software are expensive, and the installation may require the services of a technician.

(b) **Requires Administrative Time**: Proper maintenance of a networks requires considerable time and expertise. Many organizations have installed a network, only to find that they did not budget for the necessary administrative support.

(c) Sever Breakdown: Although, a server is no more susceptible to failure than any other computer, when the server "goes down" the entire network may grind to a halt. When this happens, the entire organization may lose access to necessary programs and data.

(d) Cables May Break: There is the possibility of network cable being tampered with. Some networks configurations are designed to minimize the inconvenience of a broken cable; with other configurations, one broken cable can affect the entire network.

3.2 COMPUTER NETWORK HARDWARE COMPONENTS

Networking hardware includes all computers –servers and workstations, peripherals, interface cards and other equipment needed to perform data-processing and communications such as switches, repeaters, bridges and routers.

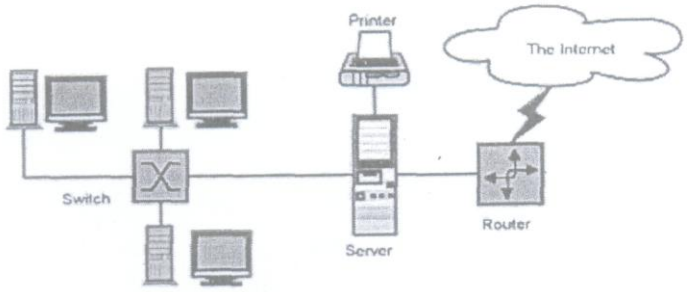


Figure 1.20: Computer Network Hardware Components

3.2.1 FILE SERVERS:

A files server stands at the heart of most networks. It is a very fast computer with a large amount of Random Access Memory (RAM) and storage space, along with a fast networks interface card. The networks operating system software resides on this computer, along with any business applications and data files that need to be shared.

The file server controls the communication of information between the nodes or workstations on a network. For example, it may be asked to send a word processor program to one workstations, receive a database file form another workstation, and store an e-mail message during the same time period. This requires a computer that can store a lot of information and share it very quickly. A server computer shares its resources, such as peripherals and file storage, with the users' computers, called clients, on a network.

Many large enterprises employ numerous servers to support their needs. A collection of servers in one location is often referred to as a server farm. It is possible to configure the machines to distribute tasks so that no single machine is overwhelmed by the demands placed upon it (called load balancing).

Students can also work cooperatively through the network. File servers should have at leas the following characteristics or configuration:

(i) 800 megahertz or faster microprocessor (Pentium 3 or 4);

(ii) A fast hard disk with at least 120 gigabytes of storage

(iii) A RAID (Redundant Array of Inexpensive Disks) to preserve data after a disk casualty.

(iv) A tape back-up unit (i.e. DAT, JAZ, Zip, or CD-RW drive)

(v) Numerous expansion slots

(vi) Fast network interface card

(vii) At least of 512 MB of RAM

3.2.2 WORKSTATIONS

All of the user computers connected to a network are called workstations or clients. A typical workstations is a computer that is

configured with a network interface card, networking software and the appropriate cables. Workstations do not necessarily need floppy disk drives because files can be saved on the file server. Almost any computer can serve as a network workstation.

3.2.3 NETWORK INTERFACE CARDS

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICS are internal, with the card fitting into an expansion slot inside the computer.

Network interface cards are a major factor in determining the speed and performance of a network. The three most common network interface connections are Ethernet cards, LocalTalk connectors, and Token Ring cards. According ton an International Data Corporation study, Ethernet is the most popular, followed Token Ring and LocalTalk.

(i) Ethernet Cards: Ethernet cards are usually purchased separately, although many computers now include an option for a pre-installed Ethernet card. Ethernet cards contain connections for either coaxial or twisted pair cables (or both) (see figure 1.21). If it is designed for coaxial cable, the

connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection.

(ii) LocalTalk connectors: LocalTalk is Apple's built-in solution for networking Macintosh computers. It utilizes a special adapter box and a cable that plugs into the printer port of a Macintosh. A major disadvantage of LocalTalk is that it is slow in comparison to Ethernet.

(iii) Token Ring cards: Token Ring network cards are similar to Ethernet cards. One visible difference is the type of connector on the back end of the card. Token Ring cards generally have a nine pin connector to attaché the card to the network cable.

3.2.4 SWITCHES/HUBS

When connecting the computers together on a network, they are not plugged into each other. Instead, each computer plugs into a separate device called a hub. Years ago, hubs were expensive devices – expensive enough that most do it- - yourself networks who were building small networks opted for coax cable instead of twisted – pair, because networks wired with coax cable do not require hubs.

A switch is simply a more sophisticated type of hub. Because the cost of switches has come down dramatically in the past few years, new networks are built with switches rather than hubs. If an older network that uses hubs and seems to run slowly, improve the networks speed by replacing the older hubs with newer switches.

Switches are more efficient than hubs, but not just because they are faster.

Hub and switches compared

Differences between a hub and a switch:

(i) In a hub, every packet than arrives at the hub or any of its ports is automatically sent out on every other port. The hub has to do this because it doesn't keep track of which computer is connected to each port. For example, suppose computer A is connected to port 1 on an 8–port hub, and computer B is connected to port 5. If computer A sends a packet of information to computer B, the hub receives the packet on port 1 and then sends it out on port 2-8. All the computers connected to the hub get to see the packet so they can determine whether or not the packet was intended for them.

(ii) A switch does kept track of which computers is connected to each port. So if computer A on port 1 sends a packet to computer B on port 5, the switch receives the packet on port 1 and then sends the packet out only on port 5. This is not only faster, but also improves the security of the system because other computers are not shown packets that are not meant for them.

(iii) Most switches are active, that is they electrically amplify the signal as it moves from one device to another. Switches are:

- Usually configured with 8,12, or 24RJ-45 ports
- Often used in a star or star-wired ring topology
- Sold with specialized software for port management
- Usually installed in a standardized metal rack that also may store network modems, bridges, or routers.

3.2.5 REPEATERS

A signal loses strength as it passes along a cable over long distances. Such loss of strength of signal is referred to as attenuation. Repeaters help to overcome attenuation. The repeater electrically amplifies the

signal it receives and rebroadcasts it. They are used when the total length of network cable exceeds the allowable distance required for that cable usually 100m.

A good example of the use of repeaters would be in base stations located in various directions of telephone network operators to boost telephony signals.

3.2.6 BRIDGES

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to –date, a bridge can connect the two. A bridge monitors the information traffic on both sides of the network so that it can pass information to the correct location. Most bridges can “listen’ to the network and automatically figure out the address of each computer on both sides of the bridge. The can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. You might say that the bridge is like a traffic cop at a busy intersection during rushhour. It keeps information

flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be sued to connect different types of cabling, or physical topologies.

ROUTERS

A router translates information from one network to another; it is similar to a super intelligent bridge. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know hen to direct traffic along back roads and shortcuts.

While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even “listen” to the entire network to determine which sections are busiest – they can then redirect data around those sections until they clear up.

If you have a network that you want to connect to the Internet, you will need to purchase router. In this case, the router serves as the translator between the information on your network and as the translator between the information on your network and the Internet.

It also determines the best route to send the data over the Internet. Routers can:

(i) Direct signal traffic efficiently;

(ii) Route messages between any two protocols;

(iii) Route messages between linear bus, star, and star-wired ring topologies; and

(iv) Route messages across fibre optic, coaxial and twisted-pair cabling.

3.3 COMPUTER NETWORK CABLING

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with networks. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types.

The types of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following are the types of cables used in networks and other ICT installations:

(a) Coaxial cable;

(b) Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) Cable;and

(c) Fibre Optic Cable

3.3.1 COAXIAL CABLE

Coaxial cabling has a single copper conduction at its centre. A plastic layer provides insulation between the centre conductor and a braided metal shield (figure 1.23). the metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

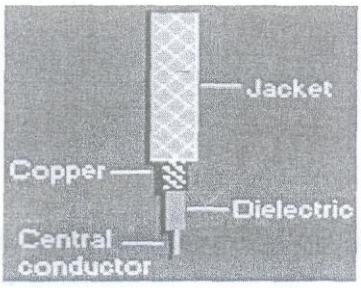


Figure 1.23: Coaxial Cable

Although, coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

(i) Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UPT) is the most popular and is generally the best option for school networks (figure 1.24).

The quality of UTP may vary from telephone –grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacjet.

Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greatest the costs per foot.

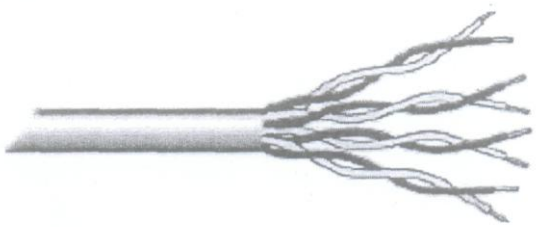


Fig.1.24: Unshielded twisted pair

(ii) Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone–style connector (fig. 1.25). A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

(iii) Shielded Twisted Pair (UTP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference; however, the extra shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology

3.3.2 FIRBRE OPTIC CABLE

Fibre optic cabling consists of a centre glass core surrounded by several layers of protective materials (fig. 1.26). It transmits light rather than

electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between building, due to its immunity to the effect of moisture and lightening.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify.

Figure 1.26: Fiber Optic Cable

3.4 TYPES OF COMPUTER NETWORK

The three basic types of networks include:

(a) Local Area Networks (LAN)

(b) Metropolitan Area Networks (MAN)

(c) Wide Area Networks (WAN)

3.4.1 LOCAL AREA NETWORK (LAND)

A Local Area Network is a network that is confined to a relatively small area. It is generally limited to a geographic area such as an office or offices within a building. Rarely are LAN computers more than a mile apart.

In a typical LAN configuration, one computer is designated as the file server. It stores all the softwares that control the network, as well as the softwares that can be shared by the computers on the network. Computers connected to the file server are called workstations. The workstations can be of less capacity than the file server, and they may have additional softeware on their hard disks. On most LANs, cables are used to connect the computers.

3.4.2 METROPOLITAN AREA NETWORKS (MAN)

A metropolitan Area Network (MAN) is a large computer network usually spanning a campus or a city. They typically use wireless infrastructure

or optical fiber connections to link their sites. For instance a university or college may have a MAN that joins together many of its LANs, situated within each department. Then from their MAN they could have several wide area network (WAN) links to other universities or the Internet.

3.4.3 WIDE AREA NETWORK (WAN)

A wide area network or WAN is a computer network covering a wide geographical area. This is different from metropolitan area networks (MANS) or local area networks (LANS). The best example of a WAN is the Internet. WANS are used to connect local area networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private, others, built by Internet services providers provide connections from an organization's LAN to the Internet. WANs are most often built of leased lines. At each end of the leased line, a router connects to the LAN on one side and a hub within the WAN on the other.

Wide Area Networks (WANs) connect larger geographic areas, such as states, Countries or the world, dedicated transoceanic cabling or satellite links are used to connect this type of network. Using a WAN, a

bank can connect all its branches nationwide into a single private network. Multinationals also connect their locations across the globe into a single private WAN. A WAN could become so complex, sing several devices to connect LANs and MANs into a global communications networks like the Internet. To users, however, a WAN will not appear to be much different from a LAN or a MAN.

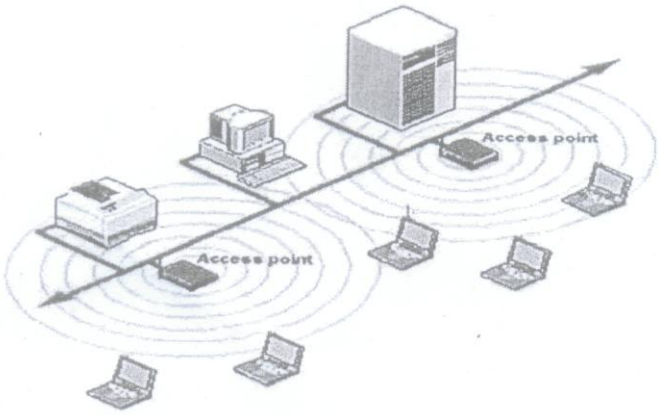


Fig 1.27: Wireless LAN

3.5 WIRELESS LANS

Not all networks are connected with cabling; some networks are wireless. Wireless LANs use high frequency radio signals, infrared light beams, or lasers to communicate between the workstations and the file server or hubs. Each workstation and file server on a wireless network has some sort of transceiver/antenna to send and receive the data.

Information is relayed between transceivers as if they were physically connected. For longer distance, wireless communications can also take place through cellular telephone technology, microwave transmission, or by satellite.

3.5.1 WIRELESS LAN

Wireless networks are efficient for allowing laptop computers or remote computers to connect to the LAN. Wireless networks are also beneficial in older buildings where it may be difficult or impossible to install cables. The two most common types of infrared communications used in schools are line-of-sight and scattered broadcast. Line-of-sight communication means that there must be an unblocked direct line between the workstation and the transceiver. If a person walk within the line-of-sight while there is a transmission, the information would need to be sent again. This kind of obstruction can slow down the wireless network.

Scattered infrared communication is a broadcast of infrared transmissions sent out in multiple directions that bounces off walls and ceilings until it eventually hits the receiver. Networking communications with laser are virtually the same as line-of-sight infrared networks.

Wireless LANs have several disadvantages. They provide poor security, and are susceptible to interference from light and electronic devices. They are also slower than LANs using cabling.

SELF ASSESSMENT EXERCISE

- Carefully list some of the advantages of routers

4.0 CONCLUSION

Unit 1 of module two has introduced you to computer networks, types of computer networks, advantages and disadvantages. You have also learnt about computer network cabling – coaxial cable, unshielded twisted pair and fibre optic cable.

5.0 SUMMARY

Computer network can be simply defined as the interconnection of stand alone computers by various means of communication. The main reasons for using a network is sharing of resources. This includes hardware and information. Some hardware commonly shared in network including printers, fax – modem and hard disk.

The network configuration/types of networks – Local Area Network, Wide Area Network and Metropolitan Area Network.

The type of cable chosen for a network is related to the network topology, protocol and size.

6.0 TUTOR MARK ASSIGNMENT

- List and explain the three types of networks you know.

Answer to self assessment exercise

Apart from a router serving as the translator between the information on your network and the internet, routers can:

- Direct signal traffic efficiently
- Route messages between any two protocols
- Route messages between linear bus, star, and star-wired ring topologies and
- Rout messages across fibre optic, coaxial and twisted pair cabling.

7.0 REFERENCE/FURTHER READING

Rebecca T. Mercum (2005): Challenges in Forensic Computing, "Communications of the ACM Vol. 48. No. 12."

Thursday Bram (2003): "What is Grid Computing Conjecture Corporation.

Scott Burns (2008): "A fresh look at cloud computing in governance".

UNIT TWO

COMPUTER NETWORK TOPOLOGY AND GENERAL E-COMMERCE

CONTENT

1.0 INTRODUCTION

A network topology is the name given to the logical arrangement or layout of computers in the network.

There are many names for each type of layouts but the following are common:

- The central or star network is a centralized network because all communication goes via the central Hub or Switch. Al the computers are connected to a central device typically a hub or switch. At the centre of the star is the hub with the network nodes located on the tips of the star.

- The mesh network also known as distributed network is a set of autonomous independent computer systems, interconnected so as to permit interactive resource sharing between any pair of the system.

- The major advantages of a client/server network is it s scalability, centralized etc.

Electronic commerce or e-commerce consists of the buying selling, marketing and servicing of products or services over computer networks, especially over the internet.

2.0 OBJECTIVES OF THE UNIT

At the end of this unit, you are expected to:

- Define and explain computer network topology
- Discuss the major physical topologies used in computer networks
- Identify the advantages of a linear bus topology, and star topology.
- Briefly state some of the disadvantages of a tree topology.
- Explain the various types of network topology
- Examine the idea behind general e-commerce framework
- Define e-commerce.
- Dilate succinctly the e-commerce relationships and e-business

3.1 COMPUTER NETWORK TOPOLOGY

The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations. Network topology is determined

only by the configuration of connections between nodes. The following subsections discuss the physical topologies used in computer networks.

3.2 THE PHYSICAL TOPOLOGIES USED IN COMPUTER NETWORKS

3.2.1 LINEAR BUS TOPOLOGY

A linear bus topology consists of a main run of cable with a terminator at each end (figure 1.2.28), All nodes (file server, workstations and peripherals) are connected to the linear cable. Ethernet and Local Talk networks use a linear bus topology.

Advantages of a linear Bus Topology

(a) Easy to connect a computer or peripheral to a linear bus.

(b) Requires less cable length than a star topology.

Disadvantages of a linear Bus Topology

(a) Entire network shuts down if there is a break in the main cable.

(b) Terminators are required at both ends of the backbone cable.

(c) Difficult to identify the problems if the entire network shuts down.

(d) Not meant to be used as a stand-alone solution in a large building.

3.2.2 STAR TOPOLOGY

A star topology is designed with each node (file server, workstations and peripherals) connected directly to a central network hub or concentrator (figure 1.28).

The star topology reduces the chance of network failure by connecting all of the systems to a central hub. This central hub rebroadcasts all transmissions received from any peripheral node to all peripheral nodes on the network, sometimes including the originating node. All peripheral nodes may thus communicate with all others by transmitting to, and receiving from, the central node only. The failure of a transmission line linking any peripheral node to the central node will result in the isolation of that peripheral node from all others, but the rest of the systems will be unaffected.

Data on a star network passes through the hub or concentrator before continuing to its destination. The hub or concentrator manages and controls all functions of the network. This configuration is common

with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

Advantages of a Star Topology

(a) Easy to install and wire

(b) No disruptions to the network when connecting or removing devices.

(c) Easy to detect faults and to remove parts.

Disadvantages of a Star Topology

(a) Requires more cable length than a linear topology.

(b) If the hub or concentrator fails, nodes attached are disabled.

(c) More expensive than linear bus topologies because of the cost of the concentrators.

3.2.3 TREE TOPOLOGY

A tree topology combines characteristics of linear bus and star topologies. It consist of groups of star- configured workstations connected to a linear bus backbone cable (figure 1.28). Tree topologies allow for the expansion of an existing network, and enable organizations to configure a network to meet their needs.

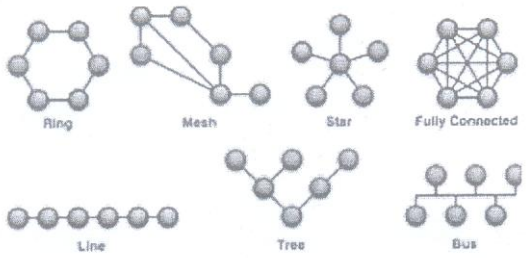


Figure 1.28: Network Topologies (Linear, Tree, etc)

Advantages of a Tree Topology

(a) Point- to-point wiring for individual segments

(b) Supported by several hardware and software vendors.

Disadvantages of a tree topology

(a) Overall length of each segment is limited by the type of cabling used.

(b) If the backbone line breaks, the entire segment goes down.

(c) More difficult to configure and wire than other topologies.

3.3 TYPES OF NETWORK

3.3.1 PEER-TO-PEER NETWORK

Peer-to-peer network allows users to share resources and files located on connected computers and to access shared resources found on other computers. However, they do not have a file server or a centralized

management source (See figure 1.29). In a peer- to- peer networks are designed primarily for small to medium local area networks. Operating system that support a peer –to-peer network include: Windows for workgroup, windows 95, windows 98, Windows XP, and Windows Vista.

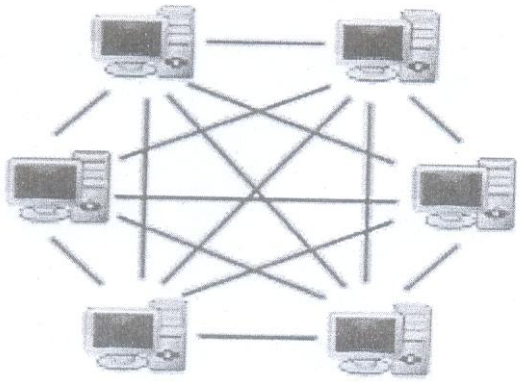


Figure 1.29: Peer-to-peer network

Advantages of a peer-to-peer network:

(a) Less initial expense – No need for a dedicated server.

(b) Setup – An operating system (such as Windows XP) already in place may only need to be reconfigured for peer –to-peer operations.

Disadvantage of a peer-to-peer network:

(a) Decentralized – No central repository for files and applications

(b) Security – Does not provide the required central security necessary in a network environment.

(c) No central administration.

3.3.2 CLIENT/SERVER NETWORK

Client/Server is a network architecture, whereby each computer or process on the network is either a client or a server. Server software generally, but not always, runs on powerful computers dedicated ford exclusive use to running the business application. Client software on the other hand generally runs on common PCs or workstations. Clients get all or most of their information and rely on the application server for things such as configuration files, stock quotes, business application programs, or to order to keep the client computer (and client computer user) free to perform other tasks.

Client/server network operating systems allows the network to centralize functions and applications in one or more dedicated file servers (See figure 1.30). The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the

mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. Novell Netware and Windows 2000 Server up to the latest Windows Server are examples of client/server network operating systems.

Advantages of a Client/Server Network

(a) centralized – resources and data security are controlled through the server.

(b) Scalability- any or all elements can be replaced individually as needs increase.

(c) Flexibility -New technology can be easily integrated into system.

(d) Interoperability –All components (client/network/server) work together.

(e) Accessibility – server can be accessed remotely and across multiple platforms.

Disadvantages of a Client/ Server Network

(a) Expense – Requires initial investment in dedicated server.

(b) Maintenance – large network will require a staff to ensure efficient operation.

(c) Dependence – when server goes down, operations will cease across the network.

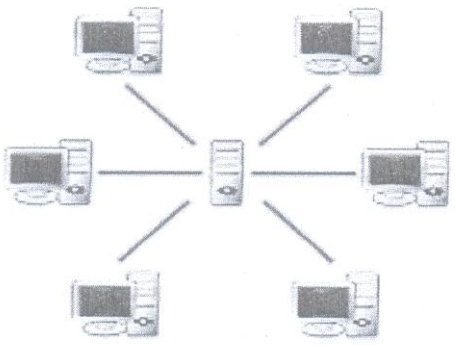


Figure 1.30: Client / Server Network

3.3.3 DISTRIBUTED PROCESS NETWORKS

A distributed processing network is one where:

(a) There are two ore more geographically separated networks

(b) These are linked by communication device such as routers, modems.

(c) The network of computers serves as a singe organization,

A large organization on many different sites may decide to have a distributed system because most of the data process and information provision is localized to each site.

Local data storage and processing is then feasible. The need for distributed computing (as distinct from several stand-alone computers) comes from the requirement that data and the results of process at one site are available to computers at other sites.

A single-site organization may also decide to have a collection of micro/minicomputers and connect these via a Local Area Network. This is possible if no large centralized processing power is needed. This is possible if no large centralized processing power is needed. It has the advantage that each node on the network can be processing, and nodes can be added to the network when needed.

Advantages of distributed processing Network

(a) Telecommunications costs between several sites are reduced provided that most of the processing is locally based.

(b) There is a greater flexibility, as additional computers can be added to the networks as needed.

(c) The organization is not reliant on a single computer, which might break down.

Disadvantages of Distributed Processing Network

(a) Commonly used data is often replicated at many sites – changes in this data, unless happening to all occurrences, can lead to an inconsistent organizational datastore.

(b) With several computers at dispersed sites, lack of standardization of equipment, software and data storage is possible.

(c) Control is more difficult.

3.4 GENERAL e-COMMERCE FRAMEWORK

INTRODUCTION

Electronic commerce is the process of doing business electronically. It is commerce accelerated and enhanced by information technology networks. It involves the automation of a variety of business –to-business and business –to-consumer transactions through reliable and secure connections, especially the internet. The internet facilitates commerce by its awesome ability to move digital information at low cost. E-commerce is necessary because it usually allows:

(a) Mass Customization: A business may give customer (business or individuals) the opportunity to tailor its products or services to the customer's (business or individual) requirements. For example, ICAN making orders for biros with some particular specifications, from their suppliers.

(b) Personalization: The idea of personalization is that the company hosting the website can know enough of its customer's preferences and fashion offers that are more likely to appeal to the customer. An example is a company presenting on its website the necessary information about what a customer may require in order to make his business judgment, instead of having several business information, which may be irrelevant to other customers.

(c) Disintermediation: This means that, with internet as a delivery vehicle, intermediate players in a distribution channel can be bypassed.

(d) Global Reach: This is the ability for every business to extend their reach to customers anywhere there is an internet connection.

3.4.1 DEFINITION OF E-COMMERCE

Electronic Commerce (EC) is a composite of technologies, processes and business strategies that foster the instant exchange of information within and between organizations. E –commerce strengthens relationship with buyers, makes it easier to attract new customers, improves (and in some cases reinvents) customer responsiveness, and opens new markets on a global scale.

Electronic Commerce is a range of applications that extend the core business activities of the enterprise into a virtual electronic community that is shared with customers, suppliers, business partners, employees and prospects.

Electronic Commerce is the application of various communications technology to provide the automated exchange of business information with internal and external customers, suppliers and financial institutions. Examples of these technologies include Electronic Data Interchange (EDI) bar coding, scanning, e-mail and fax, to name a few. Electronic Commerce, simply put, is the automation of the business process between buyers and sellers. Electronic commerce involves individuals as well as organizations engaging in a variety of electronic business transactions, without paper documents, using computer and

telecommunication networks. These networks can be either private or public, or a combination of the two.

Traditionally, the definition of electronic commerce has focused on Electronic Data Interchanged (EDI)as the primary means of conducting business electronically between entities having a pre-established contractual relationship. More recently, however, the definition of electronic commerce has broadened to encompass business conducted over the internet. This is due to the internet's surge in popularity and acceptance as a viable transport mechanism for business information. The use of a public network-based infrastructure like the internet can reduce costs and "level the playing field" for small and large businesses. This allows companies of all sizes to extend their reach to a broad customer base.

Electronic commerce or e-commerce consists of the buying, selling, marketing and servicing of products or services over computer networks, especially over the internet. In practice, this term and a newer term, e-business, are often used interchangeably. For online retail selling, the e-retailing is sometimes used.

An alternative definition of e-commerce might view it as the conduct of business commercial communications and management through

electronic methods, such as electronic data interchange and automated data-collection system. Electronic commerce may also involve the electronic transfer of information between business.

3.5 COMMERCE RELATIONSHIP

3.5.1 BUSINESS TO BUSINESS (B 2B)

Business- to- Business e-commerce (B 2B). Thousands of companies that sell product to other companies have discovered that the web provides not only a 24 hour-a- days showcase for their product but a quick way to reach the right people in a company for more information.

This is a term used to refer to companies whose customers are other businesses. It is a whole sale and supply side of the commercial process, where businesses buy, sell or trade with other business electronically. For example an automobile company, in the process of manufacturing units of its products may require some raw materials like batteries steel blades etc, which may be respetively supplied by other companies manufacturing these materials or raw materials. There may will therefore exist a network of business relationships that is referred to as supply chain.

3.5.2 BUSINESS TO CONSUMER (B2C)

This refers to the e-commerce where the company's customers are individuals who buy or transact business directly with it.

Business to Consumer (B2C) e-commerce has the following advantages:

(i) Shopping on the internet can be faster and more convenient as internet sites are open all the time. If a customer cannot find what he requires at one retail site (also known as e-tailor), a click of the mouse will take him to another in no time.

(ii) Offering and prices can change instantaneously in response to customer's demands. Customers are therefore in a position to know when to order or buy.

(iii) Call centres can be integrated with the website, interactive chatting (internet chat), customers engaged in real-time, typed exchange of information between business and one or more customer over the internet. There could also be internet telephony which is a combination of hardware and software that

uses internet as a medium for transmission of telephone calls at cheapest rates.

3.5.3 BUSINESS TO GOVERNMENT (B2G)

A new trend in E-commerce application is the B2G. Many government departments are setting up their website to directly reach the common citizen. They announce various government policies, rules and regulations on their websites. A common citizen or a business organization may interact with these webs sites to know the various details.

All the services and information for which a common citizen or business organization has to struggle from one office to another in day-to-day life, can now be accessed from one place. A citizen or business outfit may log on to the main server of the government. These serves may be kept and maintained in the individual offices of, say, Transportation, Housing, Banks, Electricity, etc The request sent to the main server will then be directed to the departmental server, and in return, the person or the organization will be informed of the desired information.

3.6 E-BUSINESS APPLICATIONS

3.6.1 Supply chain

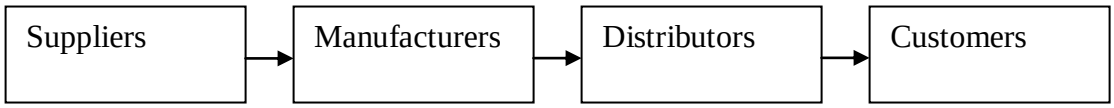
Supply chain refers to the flow of materials, payment and services from raw materials suppliers, through factory and warehouse to the end users (customers). A supply chain also include the organization and processes that create and deliver products, information and services to the end customer. It includes many tasks such as purchases, payments flow, materials handling, production, planning and control, logistics and warehousing inventory control and distribution and delivery.

3.6.2 SUPPLY CHAIN MANAGEMENT (SCM)

Supply chain management (SCM) is the oversight of materials, information, and finances as they move in a process from supplier to manufacturer to wholesaler to retailer to consumer. Supply chain management involves coordinating and integrating these flows both within and among companies. It is said that the ultimate goal of any effective supply chain management system is to reduce inventory (with the assumption that products are available when needed). As a solution for successful supply chain management, sophisticated software systems with Web interfaces are competing with Web-

applications service providers (ASP) who promise to provide part or all of the SCM services for companies who rent their services.

DOWNSTREAM FLOWS



Supply chain may be defined it as a network of facilities including:

(a) Material flow from suppliers and their "upstream" suppliers at all levels;

(b) Transformation of materials into semi-finished and finished product; and

(c) Distribution of products to customers and their "downstream" customers at all levels.

Supply chain management flows can be divided into three main flows:

(a) The product flow;

(b) The information flow; and

(c) The finances flow.

The product flow includes the movement of goods from a supplier to a customer, as well as any customer returns or services needs. The information flow involves transmitting orders and updating the status of delivery. The financial flow consists of credit terms, payment schedules, and consignment and title ownership arrangements. There are two main types of SCM software: planning applications and execution applications. Planning applications use advanced algorithms to determine the best way to file an order. Execution applications track the physical status of goods, the management of materials, and financial information involving all parties.

Some SCM applications are based on open data models that support the sharing of data both inside outside the enterprise (this is called the extended enterprise, and includes key suppliers, manufacturers, and end customers of a specific company). This shared data may reside in diverse database systems, or data warehouse, at several different sites and companies. By sharing this data “upstream” (with a company’s suppliers) and “downstream” (with company’s clients), SCM applicants have the potential to improve the time-to-market products,

reduce costs, and allow all parties in the supply chain to better manage current resources and plan for future needs.

3.7 SECURITY IMPLICATION OF E-COMMERCE

E-commerce involves mainly of three parts; search of product, price negotiation and delivery of production and payments. Making payments on the internet may take several forms using credit and debit cards, which are electronic currency. Since data pertaining to the payment is transmitted on the network from one computer to another over a communication channel, no e-commerce operation is considered one hundred percent safe. Examples of such breaches include:

a) Virus infection

b) Worms;

c) Privacy violation;

d) Hacking attacks;

e) Other intrusive actions that might shut down the network; and

f) Legal problems such as failure of either party fulfill their obligations

SELF ASSESSMENT EXERCISE

- Juxtapose between a client/server network and distributed networks in terms of their advantages.

4.0 CONCLUSION

This unit has extensively considered the concept and ideas of computer network topologies and electronic commerce. The major physical topologies used is computer network have been succinctly explained in this unit. You have also learnt about the various types of network. This unit is said to be comprehensive as it has taken you around the concept of electronic commerce and electronic business.

5.0 SUMMARY

The physical topology of a network refers to the configuration of cables, computers, and other peripherals. They are: Linear bus topology, star topology, tree or ring topology.

A typical network topology is made up of peer-to-peer, topology, client/server topology and distributed networks.

Electronic commerce is the process of doing business electronically.

The e-commerce relationship involves–Business to Business, Business to Consumer and Business to Government.

6.0 TUTOR MARKED ASSIGNMENT

- What do you understand by supply chain management?

Answer to Self Assessment Exercise

Advantages of client/server networks

• It is centralized • Scalability • Interoperability • Accessibility	• There is greater flexibility. • Organization is not related on a single computer. • Communication cost between several sites are reduced. • There are linked by communication devices such as routers modems.

7.0 REFERENCES/FURTHER READING

I. K. Oyeyinka J.O. A. Ayeni (2006): Introduction to Management Information System. Second Edition. Famorks Printers Ltd, Lagos.

Olayanju Taiwo (200): Basic Computer Studies for Schools and Colleges. Daban Printers Ltd, Lagos.

Ojajuni Jethro (2009): Computer and Business Information System. Boomark Scms Ltd (Publisher), Lagos.

UNIT THREE

COMMUNICATIONS SUPPORTED BY INFORMATION TECHNOLOGY

CONTENT

4.0 Conclusion

5.0 Summary

6.0 Tutor marked assignment

7.0 References/further reading

1.0 INTRODUCTION

Communication is the transfer of data or information on between a source and a receiver. The source transmits the data and the receiver receives it. It actual generation of the information is not part of communication nor is the resulting action of the information at the receiver.

Communication is a series of elaborate multi-sensory sign languages; signs being the words, images, audio and videos that constitute the range of presentation vehicles that, like all forms of communication have their own grammar, context (web communication).

Successful website exhibits the following features:

Webcontent, information design, user friend line and accessibility.

Short message services (Sms) is a technology that enables the sending and receiving of messages between text enabled phones. Sms first operated in Europe in 1992.

2.0 OBJECTIVES OF THE UNIT

Upon successful completion of this unit, you should be able to do the following:

- Examine the general concept of communications
- Discuss clearly and comprehensively web communication concept.
- Explain the idea behind concentrated Sms messages/Long Sms messages.
- Identify the features of a successful website.
- Analyse what make Sms messaging successful worldwide.
- Examine the different types of Sms models as discussed in the unit.
- Discuss the concept of graphic design.
- Explain the common examples of Sms alert and notification applications.

3.1.0 GENERAL CONCEPTS OF COMMUNICATIONS

Communication is the transfer of data or information on between a source and a receiver. The source transmits the data and the receiver receives it. It actual generation of the information is not part of communication nor is the resulting action of the information at the

receiver. Communication is interested in the transfer of information, the method of transfer and the preservation of the information during the transfer process.

In ancient times, a community head, say, a king, ruler, etc wishing to communicate a vital information, or call for a meeting of a certain nature would generally employ the services of a town crier designated for that function, who would in turn use a gong and a stick as a tool or channel to disseminate the required information. This means of communication is not effective in this era of rapid growth of technology. Technology has brought about changes in the methods of communication, though not without any potential risks; these methods will now form the base of our further discussion.

3.1.1 WEB COMMUNICATION

Communication is a series of elaborate multi-sensory sign languages; signs being the words, images, audio and videos that constitute the range of presentation vehicles that, like all forms of communication have their own grammar, context, and relevance as interpreted from personal experience by each member of your client-audience. Business success depends on the ability to communicate effectively to an interested audience. Driving appropriate traffic to a website is

important, but the tactics that generate visitors are not the same tactics that get visitors to stay on a website.

Websites that consistently under perform and that do not meet business expectations generally suffer because they are not designed to hold viewers attention long enough to communicate a clear concise marketing message.

3.1.2 SUCCESSFUL WEBSITES

A successful website has a well designed and clear structure with navigational options which hold and keep visitors longer than is necessary for them. This enables the visitor to easily navigate around the website and find the right information. Naturally, the text must also be clear and relevant and contain the industry, company, and product related words that the visitor may be searching for. Consequently, successful websites exhibit the following features:

(a) Webcontent

The amount of information on the internet is constantly changing. It is therefore important that visitors to a website can quickly and easily find

the information they are seeking. If a website is hard to navigate, the visitor will not stay and will look elsewhere for what they are seeking.

(b) Information design

Visitors to a site prefer to read text in their own native languages. Numerous studies show this to clearly be the case -event if more and more people speak and understand English. You can get your message across easier when the reader can read it in their own language.

The company benefits, from clear, well formulated, and well structured information that is presented in a language that the user can understand and feel comfortable with.

(c) User friendliness and accessibility

Visitors to a website determine if they have found what they are looking for in a matter of seconds. If they do not find the right information they will keep looking elsewhere. It is important, therefore, that website are both easy to sue and navigate and that the information they contain is well structured. A clear and easy-to-user website results in interested visitors who stay longer and read more.

The Web has brought information to our fingertips in an extraordinary manner over the last few years. Commercial online stores with effective websites have made the drudgery of shopping for presents a chore that can now be accomplished with ease. Many of these sites are created by teams of programmers and content writers. But what are the considerations for a small business just getting started? How do they design a site that effectively communicate their message? Large companies work with advertising agencies and pay millions for their expertise. Large consulting companies cater to the needs of the large companies work with advertising agencies and pay millions for their expertise. Large consulting companies cater to the needs of the large corporations. Small business are either on their own or work with Web developers whose expertise may lie either in their programming or graphic arts area. Web developers with expert communication skills are available, but not readily available, and usually come at a cost beyond the budget of a small business.

The Web site is a picture of how you want to be seen. As an individual with specific talents, a corporate –looking Web site may not present the picture that will be comfortable for your prospective customers. On the other hand, an overly-friendly, folksy site can project an image that appears unprofessional.

3.1.3 GRAPHICS DESIGN

Graphics are important because they are the first items that potential customers see. They need to be presented Well and need to be balanced with the rest of the page. They need to represent what is important to you and your potential clients. Graphical content needs to be consistent with the message of the site. Good graphical content also makes your site credible.

Content, however, is king. Words are what will matter. Your message will need to convey the trust necessary for someone to consider your products or services. The same message comes across in your Web site. How do you want to be seen? Figure 2.1 shows the home page of the famous Google website with the various contents displayed in a simple manner so that visitors to the site can access the site easily.

Communication implies at least a two-way dialogue. Can effective communication actually occur in a website? The answer is a resounding, “Yes”. One definition of communication is the following, “The art and technique of using words effectively and with grace in imparting one’s ideas.

If we break apart this definition we see that there are a few essential components. Firstly, there is an art or technique to communicating well. It is a learned skill and some people with the specific talent do it better than others. Secondly, effective communication requires that words can be understood by your audience. Avoid jargon. Pictures, Color, presentation are all important, but the essential ingredient is words.

Thirdly, words should be presented with grace. Why grace? A pleasing, charming approach is much more appealing and less offensive. Usability, or the ability of your visitors to get your content easily, is also an indicator of how graceful your design is.

Your attitude is the first thing people notice in face-to-face communication. The attitude of your Web site works in the same way. Your body language is a known factor in interpreting the message, just as a consistent image is important in Web design. The problem is that you cannot see the reaction of people who are viewing your Web site. Are they listening to what you are saying? Are they confused? Are they laughing?

We often have difficulty listening to other people because we think we know what they are going to say; we are seeking confirmation, not

information; and what is being said is often not what needs to be said. In essence, what we want visitors to think when they see the page is confirmation that they have found what they are looking for.

3.3.4 SHORT MESSAGE SERVICES (SMS)

Short Message Service, Sms-is-a technology that enables the sending and receiving of messages between text-enabled phones. SMS first appeared in Europe in 1992. It was included in the GSM (Global System for Mobile Communications) standards right at the beginning. Later it was ported to wireless technologies like Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA).

As suggested by the name “Short Message Service”, the data that can be held by an Sms message is very limited. One Sms message can contain at most 160 bytes of data, so one SMS message can contain up to 160 characters if 8-bit character encoding is used. (8-bit character encoding is suitable for encoding Latin Characters like English alphabets,) 80 characters if 16-bit Unicode UCS2 character encoding is used. (SMS text messages containing non-Latin characters like Chinese character should use 16-bit character encoding.)

SMS text messaging support languages internationally. It works fine with all languages supported by Unicode, including Arabic, Chinene, Japanese and Korean.

Besides text, SMS messages can also carrying binary data. It is possible to send ringtonns, pictures, operator logos, wallpapers, animations, business cards (e.g. VCards) and Wireless application protocol (WAP) configuration is to mobile phone with SMS messages.

One major advantage of SMS is that it is supported by all GSM mobile phones. Almost all subscription plans provided by wireless carriers include inexpensive SMS messaging services. Unlike SMS, mobile technologies such as WAP and mobile Java are not supported on many old mobile phone models.

3.3.5 CONCATENATED SMS MESSAGES/LONG SMS MESSAGES

One drawback of the SMS technology is that one SMS message can only carry a very limited amount of data. To overcome this drawback, an extension called concatenated SMS (also known as long SMS) was developed. A concatenated SMS text mesxage can contain more than 160 English characters. Concatenated SMS works like this: The sender's mobile phone breaks down a long message into smaller part

and sends each of them a single SMS Works like this: The sender's mobile phone breaks down a long message into smaller parts and sends each of them as a single SMS message. When these SMS messages reach the destination, the recipient mobile phone will combine them back to one long message.

3.1.6 WHAT MAKES SMS MESSAGING SO SUCCESSFUL WORLDWIDE

The number of SMS messages exchanged every day is enormous. SMS messaging is now one of the most important revenue sources of wireless carriers. SMS is a success all over the world because of the reasons discussed below:

(a) SMS messages can be sent and read at any time, Nowadays, almost every person has a mobile phone and carries it most of the time. With a mobile phone, you can send and read SMS messages at any time, whether you are in your office, on a bus at home.

(b) SMS messages can be sent to an offline Mobile phone. Unlike a phone call, an SMS message can be sent even when the phone is off or when in a place where the wireless signal is temporarily unavailable. The SMS system of the mobile network operator will

store the SMS message and later send it when the mobile phone is online.

(c) SMS messaging is less disturbing while you can still stay in touch. Unlike a phone call, you may not read or reply an SMS message immediately. Besides, writing and reading SMS messages do not make any noise. While you have to run out of a theater or library to answer a phone call, you do not need to do so if SMS messaging is used.

(d) SMS messages are supported by all GSM mobile phones and they can be exchanged between different wireless carriers. SMS messaging is a very mature technology. All GSM mobile phones support can exchange SMS messages with mobile users of the same wireless carrier, but also exchange SMS messages with mobile users of many other wireless carriers worldwide.

SMS is a suitable technology for wireless applications to build; here are some of the reasons that make SMS a suitable technology for wireless applications to build on:

(i) Firstly, SMS Messaging is supported by all GSM mobile phones. Building wireless applications on top of the SMS technology can maximize the potential user base.

(ii) Secondly, SMS messages are capable of carrying binary data besides text. They can be used to transfer ringtones, pictures, operator logos, wallpapers, animations, VCards, Vcals (calaendar entries), etc.

(iii) Thirdly, SMS supports reverse billing, which enables payment to be made conveniently. For example, to develop a commercial ringtone download application that charges a fee from the user for each ringtone downloaded. One way to accept payment is to use a reverse billion phone number obtaining from a wireless carrier. To buy a ringtone, the user will write an ordinary SMS text message that contains the ID of the rigntone to buy and send it to the SMS application's reverse billing phone number. The SMS application will then send back one or more reverse billing SMS messages that carry the rigntone. The user will be charged a fee for the reverse billing SMS messages received. the fee will be included in the user's monthly mobile phone bill or be deducted

from prepaid card credits. Depending on the agreement all or part of the money received will be given to the software owner.

3.2 SMS MESSING MODELS

There are many different kinds of SMS applications on the market today and many others are being developed. Applications in which SMS messaging can eb utilized are virtually unlimited. Some common examples of SMS messaging models are listed below:

3.2.1 PERSON –TO-PERSON TEXT MESSAGING

This is the sending of SMS from one person to another. It is the most populat usage of SMS messaging.

3.2.2 PROVISION OF INFORMATION

A popular application of the SMS technology other than person-to-person text messaging is the provision of information to mobile users. Many content providers make use of SMS text messages to send information such as news, weather report and financial data to their subscribers. Many of these information services are not free. Reverse billing SMS is a common way used by content providers to bill their users.

3.2.3 DOWNLOADING

SMS messages can carry binary data, and so SMS can be used as the transport medium of wireless downloads. Objects such as ringtones, wallpapers, pictures and operator logos can be encoded in one or more SMS messages depending on the object's size. Like information services, wireless download services are usually not free and reverse billing SMS is a common way used by content providers to bill their customers. The object to be downloaded is encoded in one or more reverse billing SMS messages. The mobile user who requests the object will be charged a certain fee for each reverse billing SMS message received.

3.2.4 ALERTS AND NOTIFICATION

SMS is a very suitable technology for delivering alerts and notifications of important events. This is because of two reasons:

(i) A mobile phone is a device that is carried by its owner most of the time. Whenever an SMS text Message is received, the mobile phone will notify you by giving out a sound or by vibrating. You can check what the SMS text message contains immediately.

(ii) SMS technology allows the "push" of information. This is different from the "pull" model where a device has to poll the server regularly in order to check whether there is any new information applications, since it wastes bandwidth and increases server load.

Some common examples of SMS alert and notification applications are described below:

- **Email, Fax and Voice Message Notifications**

In an email notification system, a server sends a text message to the user's mobile phone whenever an email arrives at the inbox. The SMS text message can include the sender's email address, the subject and the first few lines of the email body. An email notification system may allow the user to customize various filters so that an SMS alert is sent only if the email message contains certain keywards or if the email message contains certain keywords or if the email sender is an important person. The user cases for fax or voice message are similar.

- **E-Commerce and Credit Card Transaction Alerts**

Whenever an e-commerce or credit card transaction is made, the server sends a text message to the user's mobile phone. The user can known immediately whether any unauthorized transactions have been made.

- **Stock Market Alerts**

In a stock market alert application, a program is constantly monitoring and analyzing the stock market. If a certain condition is satisfied, the program will send a text message to the user's mobile phone to notify him/her of the situation. For example, an alert system can be configured such that if the stock price of a company is lower than a certain value or drops by a certain percentage, an SMS alert is sent.

- **Remote System Monitoring**

In a remote system monitoring application, a program (sometimes' with the help of a group of sensors) is constantly monitoring the status of a remote system. If a certain condition is satisfied, the program will send a text message to the system administrator to notify him/her of the situation. For example, a program may be written to "ping" a server regularly. If no response is received from the server, the program can

send an SMS alert to the system administrator to notify him/her that the server may be down.

3.2.5 SMS Marketing

SMS messaging can be used as a marketing tool. An example is an SMS newsletter system. After singing up, the user will receive SMS text messages about the latest discount and product of the company. If the user has any questions or comments, he/she can send a text message back with the questions or comments in it. The company may include its phone number in the SMS newsletter so that the user can talk to the customers services staff directly if necessary.

3.3 SMS CENTRE (SMSC)

An SMS centre (SMSC) is responsible for handling the SMS operations of a wireless network. When an SMS message is sent from a mobile phone, it will reach an SMS center firs. The SMS centre then forwards the SMS messages towards the destination. An Sms message may need to pass through more then one network entity (e.g. SMSC and SMS gateway) before reaching the destination. The main duty of an SMSC is to route SMS messages and regulate the process. If the recipient is unavailable (for example, when the mobile phone is

switched off), the SMSC will store the SMS message. It will forward the SMS messages when the recipient is available.

3.4 VALIDITY PERIOD OF AN SMS MESSAGES

SMS messages is stored temporarily in the SMS centre if the recipient mobile phone is offline. It is possible to specify the period after which the SMS message will be deleted from the SMS centre so that the SMS message will not be forwarded to the recipient mobile phone when it becomes online. This period is called the validity period.

SELF ASSESSMENT EXERCISE

- Name and explain a typical example of Sms alert and notifications you know

4.0 CONCLUSION

This unit being comprehensive as it is has made a lot of effort to show to you the exposition of communications that are supported by information technology. You have also learnt about web communication, concentrated Sms messaging and long Sms messages. You have learnt about the major features of a successful website, different types of Sms models and Sms alert and Notifications.

5.0 SUMMARY

Communication is interested in the transfer of information, the method of transfer and the preservation of the information during the transfer process.

Technology has brought about changes in the methods of communication, though not without any potential risks. Successful website has the feature of–webcontent, information design, user friendsliness and accessibility.

Short message services, Sm is a technology that enables the sending and receiving of messages between text- enabled phones.

6.0 TUTOR MARKED ASSIGNMENT

* Discuss comprehensively three major reasons why Sms is considered a suitable technology to build on.

Answer to Self Assessment Exercise

Email, Fax and voice message is a very good example of Sms alert and notification system, a server sends a text messages to the user's mobile phone whenever an email an email arrives at the in box. The Sms text

message can include the senders e-mail body. An email, notification may allow the user to customize various filters so that a Sms alert is sent.

7.0 REFERENCES/FURTHER READING

I. K. Oyeyinka And J.O. Ayeni (2006): Introduction to Management Information System. Second Edition, Famorks Printers Ltd, Lagos.

Olayanju Taiwo (2005): Basic Computer Studies for Schools and Colleges. Daban Printers Ltd, Lagos.

Olajuni Jethro (2009): Computer and Business Information System. Bookmart Scms Ltd (Publisher), Lagos.

UNIT FOUR

ELECTRONIC FILES TRANSFER/SECURITY

CONTENT

1.0 INTRODUCTION

Information and communication technologies, electronic devices and system enable computers and people to be connected in order to share information resources. These technologies facilitate the transfer of electronic data or information from one place t the other, from one person to another.

Several methods of electronic file transfer include electronic data interchange, electronic file transfer through protocol. Web surfing is the method of not looking for anything of any particular importance, but just randomly going through the internet from site to site clicking on links and so forth just to pass time. Email allows individuals and groups to communicate with one another.

Owing to the reason that internet is filled with fraudulent villains that can compromise or steal without the user knowing about, digital ID signature or certificate is an installed file resident in that computer validates identity.

2.0 OBJECTIVES OF THE UNIT

At the end of this unit, you are expected to do the following:

- Explain what you understand by the term electronic files transfer
- Discuss the several methods of electronic files transfer
- Explain the information systems architecture web surfing, surfing anonymously etc.
- Examine the usefulness of e-mails.
- Look at critically digital and certificates, the needs and reasons for using digital security.
- Examine privacy and the various threats posted.
- More so, identifying secrecy issues in controlling information.

3.1.0 ELECTRONIC FILES TRANSFER

It provides a number of value added information services and facilities electronic information transfer.

Information and communication technologies, electronic devices and systems enable computers and people to be connected in order to share information resources. These technologies facilitate the transfer of electronic data or information from one place to the other, from one person to another.

There are several methods of electronic files transfer. These include:

(a) Electronic message transfer

The most common of this is the electronic mail. The objective is to allow the efficient transfer of messages of all kinds among users of networks. Voice mail is also a form of electronic messaging. The same is true of Multimedia message system, MMS, which uses still animated video images, graphics and text to send messages.

(b) Electronic data interchange

This is a direct computer –to-computer exchange of electronic information. It is really focused on transfer of electronic information, normally provide in digital documents.

3.2.0 ELECTRONIC FILE TRANSFER THROUGH PROTOCOL

This allows pieces of information to be transferred, that may not exists in print or other traditional media. The file transfer mechanism enables efficient transfer of both text and non-text characters. Commonly used protocols for this purpose are FTP, TCP/IP for the Internet.

TCP/IP protocol is well suited for data transfer and communication. The concept will be further developed in the chapter dealing with information systems architecture.

3.2.1 WEB SURFING

Web surfing is the method of not looking for anything of any particular importance, but just randomly going through the Internet from site to site clicking on links and so forth just to pass time. This is a good way to discover something new and interesting but more often than not, one just ends up spending a couple of hours. Web surfing may also be defined as visiting different website on the network aimlessly.

When surfing the web, information about the computer d being used and location can easily be recorded. With this information websites can track what sites are being visited, help a predator locate the computer, or even help a hacker find security vulnerabilities in the computer.

Information such as a computer's IP address, location, operating system, and even the internet browser can be used against a user. Surfing the web has privacy and security risks. By surfing the internet anonymously, personal information becomes hidden and protected.

3.2.2 SURFING ANONYMOUSLY

Anonymous surfing is simply browsing the World Wide Web with unknown identity. This is primarily done through what is known as an anonymous browser based proxy. These are the websites that you can use to input the address of the web page that you wish to visit, and the service will take you to that website with information such as the location of your computer and the IP address hidden from the web page. For example, when the user tries to access something on a certain part of the web, the proxy will talk to that file as an ambassador of the user, maintaining the privacy of the user. The practice of anonymous browsing can also maintain the privacy of the user from potential loggers spying on the user's connection.

A user can pay bills, shop from home, and check account balance and so on. However, identity can be stolen or privacy invaded. If there is no protection, credit cards, identity, can be stolen or privacy invaded. If there is no protection, credit cards, identity, can be at risk. It is important to be protected when surfing. Anonymous surfing provides privacy.

3.3.0 E-MAIL USES

Email allows individuals and groups to communicate with one another. It has become an important means of communication. It is widely used to send and receive letters/notes or draft. One main advantage is that these letters are delivered almost instantly. Technically, electronic mail refers to sending of documents in electronic form from one computer to another. Each person has a mail address which corresponds to the disk storage location. This is known as the user's mailbox. Messages sent to persons are stored electronically prior to (and after) after being read in the mail box. Generally, these e-mail packages are user friendly and have large number of facilities. E-mail address is usually divided into two parts comprising the name of the user and the name of the server on which the user has his address. Following are some examples of e-mail address:

Jihn_mail@yahoo.com

Mercy2009@yahoo.com.uk

Here, the first portion, jinn_ mail or mercy 2009 is called a mail id. The second half, the address of the server where this mail is registered is called the domain.

The general syntax for the mail is Username@address of server. The letter after the dot(.) denotes the type of server and its location. When message is sent over the internet, it is sent by store and forward method. This means that during its progress from sender to receiver, the message is not continuously in electronic transit but may be stored at a computer on the internet prior to being forwarded on to the next part of its journey, until it reaches the destination.

The use of e-mail provides several advantages and disadvantages over phone or postal services;

e-mail it increasingly being used in preference to paper based memo.

3.3.1 ADVANTAGES OF E-MAIL

(a) It is faster to transmit (almost immediately);

(b) It is more convenient and ecologically friendly (no paper required);

(c) There is automatic record of when the e-mail is received;

(d) It is possible _ to send the same e-mail to a number of recipients at no extra cost.

3.3.2 DISADVANTAGES OF E-MAIL

The internet is used to send messages back and forth which is great, unfortunately there are those who use it to destroy or spy into computer data or documents, which could lead to identity theft. Some of the precautions as to the use of sending and receiving E-mails one needs to take are summarized below.

When using a wireless or remote router make sure that it cannot be accessed by an outsider. There are equipment that will read your unencrypted password easily.

Here are some guides for safe e-mails:

(a) Do not reply to anyone you do not know or open a mail that has a strange title;

(b) Use messaging software's filtering tools to reject mail from frequent spammer's e-mail addresses or with certain worlds (sex, for example) in the subject line.

(c) Find out if the Internet Services Provider (ISP) has a spam blocking service. If not, sign up for a third party spam blocking service.

(d) Encrypt and digitally sign all sensitive e-mail messages.

(e) Use win-zip software to compress and password protect your attachments.

(f) To avoid cookies sent via e-mail, use e-mail client software.

(g) Do not read e-mail on a computer that does not belong to you, if it happens, erased your history on it.

(h) Do not send sensitive personal messages on your work computer.

(i) Keep the ANTIVIRUS software updated at all times

(j) Although antivirus will help, damage can be caused by software trying to use your computer as a back door; always upgrade when alerted by whoever is providing internet security.

(k) Scan the computer for virus and spyware on a daily basis. Stick to these guides makes it hard for hackers to get data very easily.

3.4 DIGITAL SIGNATURES AND CERTIFICATES

The internet is filled with fraudulent villains that can compromise or steal without the user knowing about it till it's too late.

What are digital ID's?

Digital ID signature or certificate is an installed file resident on that computer validates identity. Digital signatures are used by programs on the internet and local to the machines to confirm your identity to any third party concerned. Digital signatures have been confused with electronic signatures. Technically, digital signatures are formulated from what is referred in the message digest as the text contained in the document about to be sent to another party, some sort of codes formulated and attached to that message forms the Digital Signature of the sender. It then becomes difficult for a third party to formulates as in the case of a handwritten signature. As the message is interrupted by the man in the middle and for a reply attack, the digital signature losses its originality and will not match one contained in the accompanying digital certificate, thus, an indication of interference.

Digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Authentic

means that the document's origin is known and that it has not been altered in any way since creation.

Digital signatures rely on certain types of encryption to ensure authentication. Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only other computer will be able to decode. Authentication is the process of verifying that information is coming from a trusted source. These two processes work hand in hand for digital signatures.

Digital Certificates

Digital certificate, bind an identity to a pair of electronic keys that can be used to encrypt and sign digital information. A Digital Certificate makes it possible to verify someone's claim that they have the right to use a given key, helping to prevent people from using phony keys to impersonate other users. Used in conjunction with encryption, Digital Certificate provide a more complete security solution, assuring the identity of all parties involved in a transaction.

A digital certificate is issued by a Certification Authority (CA) and signed with the CA's private key.

A digital certificate typically contains the:

(a) Owner's public key

(b) Owner's name

(c) Expiration date of the public key

(d) Name of the issuer (the CA that issued the digital certificate)

(e) Serial number of the digital certificate

(f) Digital signature of the issuer

3.4.1 NEED FOR A DIGITAL CERTIFICATE

Virtual malls, electronic banking, and other electronic services are becoming more commonplace, offering the convenience and flexibility of round-the –clock service direct from home. However, concerns about privacy and security might be preventing people from taking advantage of this new medium for personal business. Encryption alone is not enough, as it provides no proof of the identity of the sender of the encrypted information. Without special safeguards, there is a risk being impersonated online. Digital Certificates address this problem, providing an electronic means of verifying someone's identity. Used in conjunction with encryption, digital certificate provide a more complete security solution, assuring the identity of all parties involved in a transaction. Similarly, a secure server must have its own digital

certificate to assure users that the server is run by the organization it claims to be affiliated with and that the content provide is legitimate.

Digital certificate can be used for a variety of electronic transactions including e-mail, electronic commerce, groupware and electronic funds transfer. Netscape's popular Enterprise server requires a digital certificate for each secure server.

For example, a customer shopping at an electronic mall run by Netscape's server software requests the digital certificate of the server to authenticate the identity of the mall operator and the content provided by the merchant. Without authenticating the server, the shopper should not trust the operator or merchant with sensitive information like a credit card number. The digital certificate is instrumental in establishing a secure channel for communicating any sensitive information back to the mall operator.

3.4.2 REASONS FOR USING DIGITAL SECURITY

(a) It ensures by means of verification and validation that the user is whom he/she claims to be. This is done by combing the users credential to the digital certificate and in turn this method uses one point of authentication.

(b) Digital certificate ensure data integrity giving the user piece of mind that the message or transaction has not been accidentally or maliciously altered. This is done cryptographically

(c) Digital certificate ensure confidentiality and ensure that messages can only be ready by authorized internet recipients.

(d) Digital certificates also verify date and time so that senders or recipients can not dispute if the message was actually sent or received.

Users A as depicted above has two keys a public key, this key is available to the public for download and a private key, this key is not available to the public. All keys are used to encrypt information. This means that the keys are reversible, that is, if a private key is used to encrypt a message, the public key must be used to decrypt and vice versa.

Another user can encrypt the data using users A's Public Key. User A will use the Private Key to decrypt the message. Without user A's Private Key the data can not be decrypted.

Digital signature can be used to make documents e-mails and other data private. Someone is out there and choosing a high encryption mechanism ensures that any one attempting data would find it unviable to attempt decryption.

Users A's machine digests the data into a simple string of code after user A's software has encrypted the message digest with his private key. The result is the digital signature. User A's software then appends the digital signature to document. All of the data that was hashed has been signed. User A then passes the digitally signed document to user B.

First user B's software decrypts the signature, using User A's public key then changing it back into a message digest. After the decryption if it has decrypted the data to digest level then verifies that user A in fact did sign the data. To stop fraud certificate authorities have been introduced. Certificate authorities can sign User A's public key, ensuring that no one else uses Bobs information or impersonated his key.

If a user is uncertain of the digital signature it is possible to verify the digital signature with the certificate authority. Signatures can also be revoked if they are abused or if it is suspected that they are abused.

When a digital signature is compromised the user that suspects that the certificate is compromised should report the incident to the certificate authority.

The process of checking the validity of digital signature:

(a) User A sends a signed document to User B.

(b) To verify the signature on the document, user B's application first uses the certificate authority's public key to check the signature on user A's certificate.

(c) Successful de-encryption of the certificate proves that the certificate authority created it.

(d) After the certificate is de-encrypted, user B's software can check if user A is in good standing with the certificate authority and that all of the certificate information concerning user A's identity has not been altered.

(e) User B's software then taken user A's public key from the certificate and use it to check user A's signature. If user A's public key de-encrypts the signature successfully, then user B is assured that the signature was created using user A's

private key, for the certificate authority has certified the matching public key.

(f) If the signature is found to be valid, then we know that an intruder didn't try to change the signed document.

3.4.3 THE IMPORTANCE OF KEY REVOCATION

At time there may be grounds for believing that a private key may have been compromised. This will then result in the key pair being revoked. When a digital signature is revoked the user that is requesting to revoke needs to be verified. If a key is wrongfully revoked legal action can follow.

Digital signature delivers assurances that the other party will keep their part of the bargain. Knowing the identity of the other party is one way of gaining that assurance. Keys used for digital signatures are very long series of bits, which can be represented as long series of alphanumeric characters. This makes digital signatures unfeasible for an individual to remember. They must consequently be stored by a method which is suitable, portable and protected. The most likely current technology to support such storage is a chip. Smart cards, bios chips, e-prom ships found in cable modems and other types of descramblers are all

examples or primitive forms of digital signature that act as away of identifying user. No form of identification to this date is used more than digital signature to verify the existence of a user and confirmation of credential over the internet. Digital signatures in some form or other are here to stay.

3.5 PRIVACY

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes. Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm. When something is private to a person, it usually means there is something within then that is considered inherently special or personally sensitive. The degree to which private information is exposed therefore depends on how the public will receive this information, which differs between places and over time. Privacy can be seen as an aspect of security- one in which trade –offs between the interest of one group and another can become particularly clear.

People enjoy having private spaces, and want to keep them. Key aspects include the following:

(a) Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations;

(b) Privacy has multiple dimensions, including privacy of the physical person, privacy of personal behaviour, privacy of communications, and privacy of personal data. The last two are commonly bundled together as 'information privacy'.

(c) Individuals can claim that data about themselves should not be automatically available to other individuals and organizations, and that even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use; and

(d) Data surveillance is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.

3.5.1 THREATS TO PERSONAL DATA

This identifies ways in which personal data is threatened on the internet.

Transmission Insecurity

Data transmitted over the internet is subject to several risks:

(a) Might reach an unintended person or organization;

(b) It might be accessed by an unintended person or organization;

(c) It might not reach the intended recipient;

(d) Its contents might change while in transit;

(e) A message might be transmitted that purports to come from a particular sender, but does not;

(f) A sender may wrongfully deny that they sent it; and a recipient might wrongfully deny that they received it.

All of these circumstances have privacy implications, but the most common concerns are about access to content. Generally, Internet messages are transmitted 'in clear, i.e. in a form that is readily interpreted by anyone who receives or intercepts it. Moreover, the

nature of the internet is such that the message passes through between 1 and about 25 processor from the time that it leaves the sender's organization until it reaches the recipient's. the systems manager at each such site has, in principle, an opportunity to intercept messages. In practice, there appear to be very few such security breaches; but the risks exposure exists.

In order to protect against access to content, it is necessary to encrypt the data, and ensure that only the intended recipient has the means to decrypt it. Cryptography also offers means of addressing the other transmission security risks.

More Transaction Trails, of Greater Intensity

People already leave large numbers of data trails behind them. Internet transactions enables the automated maintenance of yet more trails of each person's activities and locations, including:

(a) Logs of email messages sent and received;

(b) Logs of web-pages visited (referred to by marketers as "the click trail'); and

(c) Logs of transactions using the many other internet services (such as FTP, Telnet, Internet Relay Chat (IRCs), video-phones and video-conferences).

Attempts are now being made to produce additional more sophisticated trail – generation mechanism, at the bidding of the web-servers that people visit. This mechanism is referred to as cookies.

A cookies is a record that is written onto the local drive of the web-browser, as a result of a command issued by a web-server. Each record has a long key, which is likely to be unique to a given application. When the user accesses a relevant page at a later date, the web-server causes the web-browser to read the record and transmit it to the web-server.

Personal Profile Extraction

The many existing and new trails can together be exploited to yield intensive information about each person's behaviour.

In the public sector, the –motivations are generally social control and protection of the public cause. In the private sector, consumer marketing organizations are interested in improving customer service

and their ability to manipulate customer behaviour. Consumer services organizations such as lenders and insurers are interested in protecting their own interest, through the identification and management of instance of misbehaviour and fraud, and of individuals who perpetrate them.

3.5.2 THREATS TO PERSONAL IDENTITY

Various privacy threats exist on the internet, those that threaten aspects of a person's identify are considered below:

(a) Appropriation of One's Identity

People are at risk of other people making statements and performing actions, as though they were them. This can be as simple as falsifying the From: address in an email. It can also be as complex as the modern, largely American phenomenon of 'identity theft'.

Identity theft is the acquisition and use of sufficient evidence of identity relating to a particular person that the thief can operate as though they were that person. This can be as simple as stealing a wallet or purse, with or without passing the contents via an intermediary or 'fence'. Alternatively, it can be achieved by mail theft,

the 'fishing' of credit card slips and loan or credit applications from rubbish-bins, or through an 'inside job', e.g. at a financial institution.

(b) Appropriation of One's Electronic Mailbox

An internet user is at risk of other people sending messages, and quite possibly lots of messages, to their electronic mailbox, which are not interesting, and which waste their time, attention –span and money.

(c) Internet Transaction Identification

In general (and with some qualifications), each email message that a person sends identifies them to the recipient. In some circumstances, this may represent a privacy risk. This arises wherever the sender anticipates physical risk to themselves if their identity becomes apparent, as occurs with 'whistleblowers', and witnesses of serious crimes.

In general (and with some qualifications), each access a person makes to a web-server identifies several things about them to that machine and its masters; for example, the web-server generally provides the web-server with its identity (the IP-address'), to enable the requested page to be sent to it.

Additional information about the sender may be disclosed (generally without the person being aware of it). This can be achieved through the use of cookies, or the application of powerful client-side programming languages, such as the relatively well-behaved Java, and the dangerous Active – X.

(d) Location Services

The internet provides an enhanced means whereby people and organizations can find one another. This has dramatic power, because it combines a vast array of pre-existing data-sources (such as telephone books) with new source (such as e-list and newsgroup achieves), and makes them all available to search engines.

Such services are a great boon to people who have socially acceptable reasons for wanting to find other people. In some circumstances it can be annoying or unpleasant. In some situations, it may be life-threatening.

(e) The Possibility of Routine Self-Identification

Information technologies have been generating technological and marketing imperative towards individuals being expect to identify

themselves on a routine basis, when conducting transactions that have hitherto been anonymous or pseudonymous. Some electronic commerce and electronic service delivery technologies on the internet add to that pressure.

This is threatening to the private space of even those who have nothing to hide; and much more sinister to those many people who have experience repression from other individuals, organizations.

3.6 SECRECY ISSUES

Secrecy involves norms about the control of information, whether limiting access to it, destroying it, or prohibiting or shaping its creation.

Secrecy is a general and fundamental social process known to all societies. It can characterize interaction at any level –from information an individual withholds, to secret rites of passage of pre-industrial societies, to the secrets of contemporary franternal or business organizations, to state-held information on national security.

Secrecy norms are embedded in role relationships and involve obligations and rights to withhold information, whether reciprocal or singular.

In a generic sense, security is “freedom from risk or danger”. In the context of computer science, security is the prevention of, or protection against:

(a) Access to information by unauthorized recipients

(b) Intentional but unauthorized destruction or alternation of that information. Security may also be defined as the ability of a system to protect information and system resources (which include CPUs, disks, and programs, in addition to information) with respect to confidentiality and integrity.

3.6.1 THREAT TO INFORMATION SYSTEM

Most common threats to computerized information systems include:

(a) Hardware failure
(b) Software failure;
(c) Personnel actions;
(d) Workstation access penetration
(e) Theft of data, services and equipment;
(f) Electrical problems
(g) User errors

(h) Program changes; and

(i) Telecommunication problems.

These threats can stem from technical, organizational and environmental factors compounded by poor management decisions.

Computerized or automated information systems are especially vulnerable to such threats for the following reasons:

(a) A complex information system cannot be replicated manually. Most information cannot be printed or is too voluminous to be handled manually.

(b) There is usually no visible trace of changes in computerized systems because computer records can be read only by the computer.

(c) Computerized procedures appear to be invisible and are not easily understood or audited.

(d) The development and operation of automated systems require specialized technical expertise, which cannot be easily communicated to end users. Systems are open to abuse by highly

technical staff members who are not well integrated into the organization. (Programmers and computer operators can make unauthorized changes in software while information is being processed or can use computer facilities for unauthorized purposes. Employees may make unauthorized copies of data files for illegal purpose.)

(e) Although the chances of disaster in automated systems are no greater than in manual systems, the effect of a disaster can be much more extensive. In some cases, all the system's records can be destroyed and lost forever.

(f) Most automated systems are accessible by many individuals. Information is easier to gather but more difficult to control.

(g) On-line information systems are even more difficult to control because data files can be accessed immediately and directly through computer terminals. By obtaining valid user's logon IDs and passwords, unauthorized access to or manipulation of data in on-line systems are considerably higher than in the batch environment.

The security of information system is maintained by measures taken to prevent threats to these system or to detect and correct the effects of any damage. Information system security aims to protect corporate assets or, at least, to limit their loss.

SELF ASSESSMENT EXERCISE

* Briefly explain ways in which personal data is threatened on the internet.

4.0 CONCLUSION

Electronic files transfer provides a number of value added information services and facilitates electronic information transfer. In this unit, you have learnt about the various methods of electronic files transfer, the information systems architecture, the advantages and disadvantages of e-mails you have also got to understand why there is need for a digital certificate and digital security.

5.0 SUMMARY

Several methods of electronic files transfer include e-Electronic message transfer, electronic data interchange and electronic transfer through protocol. The later concept further buttress information systems

architecture–web surfing, surfing anonymously. Emails allow individuals and groups to communicate with one another. It is faster to transmit (almost immediately). Digital signatures are used by programs on the internet and local to the machines to confirm your identity to any third party concerned.

Secrecy involves norms about the control of information, whether limiting access to it, destroying it, or prohibiting or shaping its creation.

6.0 TUTOR MARKED ASSIGNMENT

- Computerized or automated information systems are especially vulnerable to certain threats due to reasons that are considered controversial. Discuss

ANSWERS TO SELF ASSESSMENT EXERCISE

- Transaction insecurity might:

- Reach an unintended person or organization
- Be accessed by an unintended person or organization
- Not reach the intended recipient
- Might change content while in transit etc.

7.0 REFERENCE/ FURTHER READING

Jame P. Anderson (2000): “Computer security Threats and surveillance” James P. Anderson and Co.

Graham curtis (2001): Business Information System, Analyst, Design and Practice” 3rd Edition, Addision Wesly.

Ojajuni Jethro (2009): Computer and Business Information System. Boomart SCMS Ltd, Lagos.

MODULE THREE

UNIT ONE: COMPUTER CRIME AND ABUSE

UNIT TWO: COMPUTER VIRUS, WORMS, AND TROJAN, THE THREAT AND PREVENTION

UNIT THREE: INFORMATION SYSTEM ARCHITECTURE (COMMUNICATION NETWORKS)

UNIT FOUR: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

UNIT ONE

COMPUTER CRIME AND ABUSE

CONTENT

3.3.1 Interruption

3.3.2 Interception

3.3.3 Modification

3.3.4 Fabrication

3.4 Security threat and information system sources

3.4.1 Hardware

3.4.2 Software

3.4.3 Data

3.4.4 Communication lines and network

3.5 Information access security

3.5.1 Identification and authentication (1 & A)

3.5.2 Logon IDs and password

3.5.3 Features of password

3.5.4 Identification and authentication best practices

3.6 Data encryption

3.6.1 Data encryption standard (DES)

3.6.2 An overview of cryptography and digital certificates

3.7 Digital signature and digital watermarks and digital certificate

3.8 Biometric control

3.9 Firewalls and use of USB sticks, disk, memory sticks and other removable devices

1.0 INTRODUCTION

Any illegal act in which a computer is used as the primary tool is otherwise known as computer crime. Computer abuse is unethical use of a computer. Impersonation, Trojan horse method, logic bomb and computer viruses forms related computer security threats. Computer security and network security is meant to address three security requirements such as confidentiality, integrity and availability. The resources of a computer – based information system communication lines as well as networks.

Controlling access to information systems to guarantee authorized access is fundamental to information system security. A digital certificate is an electronic file that uniquely identifies individuals and web sites on the internet and enables secure, confidential communications.

2.0 OBJECTIVE OF THE UNIT

Having studied this unit very well, you should be able to:

- Define computer crime and abuse
- Examine the nature and scope of computer crime and abuse.

- Explain some of the security of a computer system and networks.
- Identify security threats and information system sources.
- Expatriate the content of information access security explain some of the features of password
- Discuss data encryption, digital certificates and biometric control.
- Differentiate between vocal identification and facial verification.

3.1.0 COMPUTER CRIME AND ABUSE

Computer crime is defined as any illegal act in which a computer is used as the primary tool. Computer abused is unethical use of a computer.

Security threats related to computer crime or abuse include:

(a) Impersonation: Gaining access to a system by identifying oneself as another person. Having defeated the identification and authentication controls employed by the system, the impersonator enjoys the privileges of a legitimate user.

(b) Trojan horse method: Concealing within an authorized program a set of instructions that will cause unauthorized actions.

(c) Logic bomb: Unuthorised instructions, often introduced with the Trojan horse technique, which stay dormant until a specific event occurs (or until a specific time comes, as the instructions may keep checking the computer's internal clock), at which time they effect an unauthorized act. The specific time or date during which the harmful action is performed is referred to as the trigger.

(d) Computer viruses: segments of codes that are able to perform malicious acts and insert copies of themselves into other programs in the system and onto the removable storage devices such as diskettes and USB-based disks placed in the infected personal computer. Because of this replication, a virus will progressively infect healthy programs and systems. Close relatives of viruses are worms which are independent programs that make and transmit copies of themselves through telecommunications networks. Computer viruses have become a pervasive threat in personal computing and are the most frequently encounter threats to end-user computing.

(e) Denial of service: Rendering the system unusable by legitimate users.

(f) Data diddling: Changing data before or during input, often to change the contents of a database.

(g) Salami Technique: Diverting small amounts of money from a large number of accounts maintained by the system. These small amount will not be noticed. It is a system of chopping off small amounts of money from an existing balance in an account and subsequently placing the chopped off amounts into an account the perpetrator can access.

(h) Spoofing: Configuring a computer system to masquerade as another system over the network in order to gain unauthorized access to the resources the system being mimicked is entitled to.

(i) Super zapping: Using a systems program that can bypass regular system controls to perform unauthorized acts.

(j) Scavenging: Unauthorized access to information by searching through the residue after a job has been run on a computer. Techniques rang from searching waste baskets or dumpsters for printouts to scanning the contents of a computer's memory.

(k) Data leakage: Variety of methods for obtaining the data stored in system. The data may be encoded into an innocuous report in sophisticated ways, for example, as the number of characters per line.

(l) Wiretapping: Tapping computer telecommunications lines to obtain information.

Some of the techniques listed above may be used for a direct gain of financial resources, others for industrial espionage, and others simply for destructive purposes. Probably the most important unrecognized threat today is the theft of portable computers, with access code and information in their memories; of equal importance are the losses due to the theft of intellectual property, such as software, produce development information, customer information or internal corporate documents.

3.2 SECURITY REQUIREMENTS

Computer security and network security address three security requirements:

(a) **Confidentiality**: Requires that the information in a computer system be accessible for reading by authorized parties only. This type of access includes printing, displaying and other forms of disclosure, including simply revealing the existence of an object.

(b) **Integrity**: Requires that computer assets can be modified by authorized parties only. Modification includes writing, changing, changing status, deleting and creating.

(c) **Availability**: Requires that computer system resources are available to authorized parties as and when they are needed.

3.3 Types of threats

The types of threats to the security of a computer –based information system are best characterized by viewing the functioning of the computer in providing information. In general, there is a flow of information from a source, such as a file or a region of main memory, to a destination such as another file or a user.

This normal flow is depicted in Figure 2.2a. The remainder of the figures shows four general categories of threats:

3.3.1 Interruption

System resources are destroyed or become unavailable or unusable. This is a threat to availability. Examples include destruction of piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file-management system.

3.3.2 Interception

An authorized party gains access to a resource. This is a threat to confidentiality. The unauthorized party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network and the illicit copying of files, or programs, keyboard loggers and data shifters.

3.3.3 Modification

An unauthorized party gains access to and tampers with the system resources. This is a threat to integrity. Examples include changing values in a data file, altering a program so that it performs differently and modifying the content of messages being transmitted in a network.

3.3.4 Fabrication

An unauthorized party inserts counterfeit objects into the system. This is also a threat to integrity. Examples include the insertion of spurious messages in a network or the addition of records to a file.

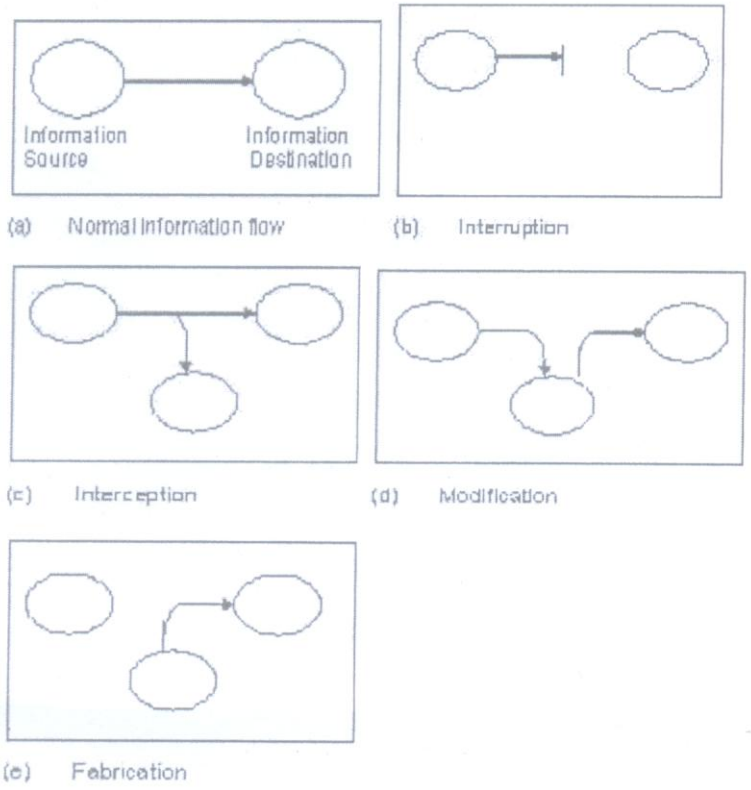


Figure 2.2 - Categories of Security Threats

3.4.0 SECURITY THREATS AND INFORMATION SYSTEM RESOURCES

The resources of a computer –based information system can be categorized as hardware, software, data and communication lines as well as networks. Figure 2.3. indicates the nature of the following threats faced by each category of asset.

3.4.1 Hardware

The main threat to computer system hardware is in the area of availability. Hardware is the most vulnerable to attack of this nature and the least amenable to automated controls. Threats include accidental and deliberate damage to equipment, as well as theft. The proliferation of personal computers and workstations and the increasing use of local are networks increase the potential for losses of this kind. Physical and administrative security measures are needed to deal with these threats.

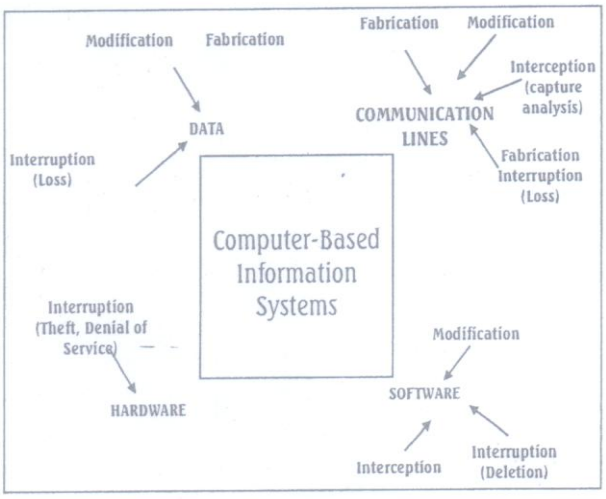


Figure 2.3 Security threats and Information Systems Assets

3.4.2 Software

The operating system, utilities, and application programs – the software - are what make computer system hardware useful to businesses and individuals. Several distinct threats need to be considered.

A key threat to software is availability. Software especially application software , is surprisingly easy to delete. Software can also be altered or damaged to render it useless. Careful software configuration management, which includes making backups of the most recent version of software, can maintain high availability.

A more difficult problem to deal with is software modification that results in a program that still functions but behaves differently after it has been tampered with by unauthorized persons. Computer viruses and related attacks fall into this category and are treated later in this chapter.

A final problem is software secrecy. Although certain countermeasures are available, by and large the problem of unauthorized copying of software has not been resolved completely at least in the third world countries.

3.4.3 Data

Hardware and software security are typically concerns of professionals in computing centers or individual concerns of users of personal computers. A much more widespread problem is data security, which involves files and other forms of data controlled by individuals, groups, and business organizations.

Security concerns with respect to data are broad, encompassing availability, confidentiality, and integrity. In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or as a result of malice.

The obvious concern with confidentiality is the unauthorized access to data files or databases, and this area has been the subject of perhaps more research and effort than any other aspect of computer security. A less obvious confidentiality threat involves the analysis of data and it manifest in the use of so –called statistical database, which provides summary or aggregate information. Presumably, the existence of aggregate information does not threaten the privacy of the individuals involved. However, as the used of statistical database grows, there is an increasing potential for disclosure of personal information. In essence, characteristics of constituent individuals may be identified through careful analysis. To take a simple example, if one table records the aggregate of the incomes of respondents, A,B,C, D, and E, the differences between the two aggregate would be the income of E. this problem is exacerbated by the increasing desire to combine data sets.

Finally, data integrity is a major concern in most installations. Modifications to data files can have consequences ranging from minor to disastrous.

3.4.4 Communication Lines and Networks

Communication systems are used for data transmission. Thus, the concerns of availability, security and integrity that are relevant to data security apply as well to network.

3.5 INFORMATION ACCESS SECURITY

Controlling access to information systems to guarantee authorized access is fundamental to information system security. Over the years, a lot of methods and technologies have been adopted and developed to ensure secure information access. These technologies and methods are discussed below:

3.5.1 Identification and Authentication (1 & A)

Identification and authentication is the process of providing one's identity. It is the means by which a user provides a claimed identity (credentials) to the system and where the credentials are authenticated by the system before providing the user access.

1 & A is a critical building block of computer security, since it is the basis for most types of access control and for establishing user accountability. U ser accountability required the linking of activities on a computer system to specific individuals and, therefore, requires

the system to identify users. It is a technical measure that prevents unauthorized people (or unauthorized processes) from entering a computer system. If users are not properly identified and authenticated, particularly in today's open-system networked environments, organizations are at a higher risk to unauthorized access.

Some of 1 & A's more common vulnerability in gaining unauthorized system access include:

(a) Weak authentication methods
(b) The potential for users to bypass the authentication mechanism;
(c) The lack of confidentiality and integrity for the stored authentication information; and
(d) The lack of encryption for authentication information transmitted over a network.

3.5.2 Logon IDs and Password

This two-phase user identification and authentication process based on something you known can be used to restrict access to computer information, transactions, programs and to the computer system itself. The computer can maintain an internal list of valid logon IDs and a

corresponding set of access rules for each logon ID. These access rules identify the computer resources the user of the logon ID can access and constitute the users' authorization. As a minimum requirement, access rules are usually specified at the operating system level (controlling access to files) or within individual application systems (controlling access to menu functions and types of data or transactions).

The logon ID provides individual identification. Each user gets a unique logon ID that can be identified by the system. The format of logon IDs is typically standardized.

The password provides individual authentication. Identification/ authentication is a two- step process by which the computer system first verifies that the user has a valid logon ID (user identification) and then requires the user to substantiate his/her identity with a password.

3.5.3 Features of passwords

(a) A password should be easy for the user to remember but difficult for a perpetrator to guess. Initial passwords may be allocated by the security administrator or generated by the system itself. When the

user logs on for the first time, the system should force a password change to improve confidentiality. Initial password assignment should be randomly generated and assigned, where possible, on an individuals and not a group basis. The ID and password should be given out in a controlled manner that ensures only the appropriate user receives this information. New accounts not used within a few days or without an initial password assignment should be suspended within the system.

If the wrong password is entered a predefined number of times, typically three, the logon ID should be automatically and permanently deactivated (or at least for a significant period of time).

(b) Passwords should be internally one-way encrypted. Encryption is a means of encoding data stored in the computer. This reduces the risk of a perpetrator gaining access to other user's passwords. (If the perpetrator cannot read and understand it, he cannot use it). Passwords should not be displayed reports in index or card files or written on pieces of paper taped inside a person's desk. These are the first place a potential perpetrator will look.

(c) Passwords should be changed periodically. On a regular basis (for example, every 30 days) the user should change his/her password.

The frequency of changing the password should depend inter alia, upon the criticality of the information access level, the nature of organization, the IS architecture and technologies used. Password should be changed by user at his/her own workstation, rather than at the administrators' terminal or in any location where the new password might be observed. The best method is for the computer system to force the change by notifying the user prior to the password expiration date. The risk of allowing the voluntary password changes is that, generally, users will not change their password unless forced to do so.

(d) Password must be unique to an individual. If a password is known to more than one person, the responsibility of the user for al activity within their account cannot be enforced.

3.5.4 Identification and authentication best practices

Logon ID requirement include:

a) Logon ID not used after a number of days should be deactivated to prevent possible misuse. This can be done automatically by the system or manually by the security administrator.

b) The system should automatically disconnect a logon session if no activity has occurred for a period of time. This reduces the risk of misuse of an active logon session left unattended, because the user went for lunch, stepped into a meeting or otherwise forgot to log off. This is often referred to as a time out.

The password syntax rules include:

(i) Ideally, passwords should be five to eight characters in length. Anything shorter is too easy to guess. Anything longer is too hard to remember.

(ii) Passwords should require a combination of at least three of the following characteristics: alpha, numeric, upper and lower case, and special characters.

(iii) Passwords should not be particularly identifiable with the user (such as first name, last name, spouse name, pet's name). some organizations prohibit the use of vowels, making word association/guessing of passwords more difficult.

(iv) The system should not permit previous password(s) to be used for at least a year after being changed.

The above rules should be applied minimally to individual with privilege system account authorities such as system administrators, security administrator. Users with privilege authorities need such access in establishing and managing appropriate system configurations. However, such privileges enable the user to bypass any access control software restrictions that may exist on the system. The general rule to apply is that the greater the degree of sensitivity of the access rights, the stricter the access controls should be.

Token devices, One-Time passwords: A two –factor authentication techniques, such as a microprocessor-controlled smart card, generates one-time passwords that are good for only one logon session. Users enter this password along with a password that has been memorized to gain access to the system. This technique involves something you have (a device subject to theft) and something you know (a personal identification number). Such devices gain their one time password status because of a unique session characteristics (such as ID or time) appended to the password.

3.6 DATA ENCRYPTION

Encryption by definition means hidden writing. Data encryption is the transformation of data into a form that is unreadable to anyone

without an appropriate decryption key. It prohibits access to information by keeping it in a form that is not intelligible to an unauthorized user. Encryption is gaining particular importance as electronic commerce over telecommunications networks is gaining momentum. Encryption renders access to encoded data useless to an intruder who has managed to gain access to the system by masquerading as a legitimate user or to an industrial spy who can employ a rather simple receiver to pick up data sent over a satellite telecommunications link. Thus, the technique is important not only in the protection of the system boundary but also in the communications and database controls.

The two most important encryption techniques are the:

(a) Private key encryption – data encryption standard (DES)

(b) Public key encryption

3.6.1 Data Encryption Standard (DES)

Data encryption standard (DES) (is scrambling data or any text in general, into a cipher that can be decoded only if one has the appropriate key (that is the bit pattern). It renders the encoded data

useless to an interloper. The major disadvantage of the DES is that keys must be distributed in a secure manner. Since the keys must be changed frequently, this represents significant exposure. A prior relationship between the sender and the receiver is also necessary in order for them to share the same private key.

In public -key systems, two keys are needed to ensure secure transmission; one is the encoding key and the other is the decoding key. Because the secret decoding key cannot be derived from the encoding key, the encoding key can be made public therefore, they do not require secure distribution of keys between parties prior to their communication. Drawback of public-key encryption and decryption is that they are more time-consuming than the private key systems, and can significantly degrade performance of transaction processing systems.

3.6.2 An Overview Of Cryptography & Digital Certificates

Encryption is the process of transforming information before communicating it to make it unintelligible to all but the intended recipient. Encryption employs mathematical formulas called cryptographic algorithm, or ciphers, and number called keys, to encrypt or decrypt information.

- Symmetric cryptography: Until recently, symmetric encryption techniques were used to secure information transmitted on public networks. Traditional symmetric cryptographic systems are based on the idea of a shared secret. In such a system, two parties that want to communicates securely first agree in advance on a single 'secret key' that allows each party to encrypt and decrepit messages.

Symmetric cryptography has several drawback. Exchanging secret keys is unwieldy in large networks. Furthermore, the sharing of secret keys requires both senders and recipients to trust, and therefore be familiar with every person they communicate with securely. Also, symmetric systems require a secure channel to distribute the 'secret' keys in the first place. if there is indeed such a secure channel, why not use it to send the entire secret message? In today's web-based systems involving many participants and transitory interactions with strong cryptography requirements, such symmetric key-based system are highly impractical as a means for agreeing upon the necessary secrets to being communicating securely.

- Asymmetric cryptography: Today's public key or asymmetric cryptography systems are a considerable improvement over traditional symmetric cryptography systems in that they allow two parties to exchange data privately in the presence of possible eavesdroppers, without previously agreeing on a "shared secret". Such a system is called "asymmetric" because it is based on the idea of a matched cryptographic key pair in which a cryptographic key is no longer a simple ' shared secret' but rather is split into two sub keys, the private key and public key.

Abstractly, a participant wishing to receive encrypted communication using an asymmetric cryptographic system will first generate such a key pair, keeping the private key portion as a secret and then "publishing" the public-key portion to all parties that would like to encrypt data for that particular. Because encrypting data requires only access to the public key, and decrypting data requires the private key, such as system in principle can sidestep the first layer of complexity in the key management problem since no shared secret need be exchanged.

- Modern cryptographic systems: A hybrid approach – in fact, a combination of public–key and traditional symmetric

cryptography is used in modern cryptographic systems. The reasons for this is that public –key encryption scheme are computationally more intensive than the symmetric but not as fast for encrypting bulk data. As a result, modern cryptographic system typically use public –key cryptography to solve the key distribution problem first, then symmetric key cryptography is used to encrypt the bulk data. Such a scheme is used today for securing web-based business transactions as well as by secure e-mail scheme that built into such products as Netscape communicator and the Microsoft Internet Explorer.

3.7 DIGITAL SIGNATURE

The asymmetric cryptosystem has paved the way for the used of a digital signature as a control mechanism. Stated simply, a digital signature is a data item that accompanies a digitally encoded message that can be used to ascertain both the originator of the message and the integrity of the message. In a sense, a digital signature functions as an integrity check-value. If a dispute arises, the digital signature must be able to serve as evidence to firmly establish the identify and authentication of the message originator. Therefore, the digital signature must be unique; that is, the recipient of the message cannot

generate a digital signature that is identical to that of the originator. An integrity check-value, on the other hand, is capable of generating the same check-value since the recipient knows the key to generate the value to begin with.

A simple digital signature scheme can be implemented using the RSA cryptosystem. The RSA cryptosystem is a public –key cryptosystem that offers both encryption and digital signatures (authentication). Ronald Riverst, Adi Shamir, and Leonard Adleman developed the RSA system in 1988; RSA stands for the first letter in each of its inventor's last names.

In implementing the digital signature scheme, the originator of the message encrypts the message with a private key to form the signature and sends it along with the plain text message. The recipient then decrypts the signature using the originators' public key, which is made known publicly, and checks to see if the decrypted text matches the plain text. If both are identical then the signature is verified. This scheme has an efficiency problem – it encrypts and decrypts the entire message and doubles the size of the message to transmit and therefore increases the processing and communication overhead.

While digital signature methodologies support authentication and data integrity, they do not provide trading partners or consumers any

degree of confidentiality. One could however if so desired, choose a symmetric algorithm to encrypt the message with a share private key in order to achieve maximum security.

a. Digital Watermarks

Digital watermarking helps conceal information to protect intellectual property rights of multimedia documents. A digital watermarks can be detected only by appropriate software and contains information regarding the origin, author, owner, usage rights, distributor or authorized user of a multimedia document. Digital watermarking is a technology complementary to the secure container technology. Combing a secure container with watermarking technology is required for a robust end – to- end electronic commerce framework.

b. Digital certification

A certificate, according to the American Heritage Dictionary, the 3rd edition, is 'a document testifying to something that is true." Its electronic counterpart, the digital certificate, is a "data structure digitally signed by some party in whom users of the certificate place their trust".

A digital certificate is an electronic file that uniquely identifies individuals and web site on the internet and enables secure, confidential communications. It associates the name of an entity that participates in a secured transaction (for example, an e-mail address or a web site address) with the public key that is used to sign communication with that entity in a cryptographic system.

Various types of digital certificate (DC) can be used in electronic commerce. The most important DC is the public –key certificate, where a public key value is securely associated with a person, an organization or other entity and a digital signature from a trusted third party, called a certification authority (CA), is present to attest to the truth of such an association.

The public-key certificate is composed of various fields carrying such information as certificate formal version, certificate serial number, signature, algorithm identifier for certificate issuer's signature, issuer's name, validity period of the certificate, the name of the subject, subjects public key and its algorithm identifier, and issuer's digital signature.

For a wide distribution of public –key certificates, a hierarchy of CA's has to be established since it is not feasible to establish one certification

authority, which can issue public-key certificates for all the public-private key pair holders globally. In order to verify a validity of a public-key, therefore, the user also needs to acquire the public -key certificate of the signing authority of the o first certificate, and all the certificate up the chain to that of the root CA.

Digital certificates also attempt to provide some assurance about the certificate holder's business. Commercial certification authorities, such as VeriSign Inc. have introduced the concept of certificate classes for different levels of assurance. Currently, VeriSign offers three classes of certificates:

(a) Class 1 certificates: Are issued to individuals only and confirm that the users' name (or alias) and e-mail address from an unambiguous subject name within the VerSign Repository. They are communicated electronically to subscribers and added to the set of available certificates. Class 1 certificates are typically used for web browsing and personal e-mail, to modestly enhance the security of these environments. They, however, do not provide authentication of the identities of the subscribers.

(b) Class 2 certificate: are currently issued to individuals to confirm that the application information provided by the subscriber does

not conflict with information in well-recognized consumer databases. Class 2 certificates are typically used for intra-and inter-organisational e-mail, small "low-risk" transactions, password replacement and so on. They provides some assurance of a subscribers' identity, based on an automated on-line process that compares the applicants' name, address, and other personal information against widely referenced databases.

(c) Class 3 certificate: are issued to both individuals and organizations. Personal appearance before a class 3 local registration authority (LRA) or its delegate (such as a notary) is required for individual applicants. Validation of class 3 certification applications for organizations include a review of pertinent records provided by the applicants or third-party business databases (such as credit reports), and an independent call-back to the organizations. These certificates are used primarily for certain electronic commerce applications such as electronic banking, electronic data interchange, software validation and membership –based online services. Individual class 3 certificate processes utilizes various procedures to obtain probative evidence of the identity of individual subscribers.

These validation procedure provide stronger assurance of an applicants' identity than Class 2 certificate. Class 3 certificates can provide assurance of the existence and name of various public – and private-sector organizations (such as government agencies and corporations). Validation of Class 3 certificate applications for organization includes review by the applicable Class 3 1A of authorization records provided by the applicant or third –party business databases, and independent call-back ("out-of-band" communications) to the organization. Class 3 certificates are used by VeriSign customers primarily for certain electronic commerce applications such as electronic banking, electronic data interchange (EDI) and membership –based on –line services.

3.8 BIOMETRIC CONTROL

The last category of authentication mechanism is based upon the unique attributes of individual-Biometrics, which uses technology to identify people by a living trait such as fingerprint recognition, voice recognition, handwriting analysis, retinal scan, and hand geometry recognition. In Australia for example, about 500 supermarkets have installed biometric technology to record the movements of thousands of staff, while the biggest consumer of biometric systems, the U.S.

Government, has used the technology to restrict access to high-security locations and to combat welfare fraud.

(a) Signatures;

(b) Fingerprints

(c) Hand geometry

(d) Faces

(e) Voices, and

(f) Eyes recognition

Biometrics can provide a higher degree of security and convenience derived from using the body as a "living" password rather than employing a PIN, or access cards, which can be lost, stolen, forgotten or even forged.

Eye Recognition

Research has established without a doubt the uniqueness of retinal and iris patterns. To date, no one has successful fooled a retina – scanning device. New devices can capture an iris image from over a meter away. Scanning devices are bulky and time-consuming.

Facial Verification

Simply put, is how most human being s identify one another. It is a natural, non-intrusive identification method that will work on just about anyone. Expression variations, changes in hair style, facial hair, glasses, movement, and angle of head all contribute to difficulties in using facial verification.

Vocal Identification

People are most comfortable and familiar speaking into a device in order to identify themselves. Voice identification is not as accurate as other methods as it tends to reject genuine users due to background noise. It is also too insecure for use in high-security markets, and too slow for customer services applications such as ATMs or phone banking.

Written Verification

Authorized users can sign a document into an electronic writing tablets and "seal" it, so it can be viewed but not tampered with. The technology is by far one of the cheapest biometrics available.

Hand reading

Hand geometry system measure the shape of the hand, which makes it deal for industries where hands may be dirty or scarred.

Such systems, however, are bulky, making them more intrusive than voice or iris recognition technology, and they are less accurate than fingerprint systems.

Finger Print System

Reads the unique pattern of lines on the tip of a finger, or compare the points where print ridges join or end. Some methods count number of ridges between points, processing the fingerprint image and recording the print's sound wave. Main drawback in the commercial sector is price. Fingerprint methodologies compete not only against other biometrics, but also against established security devices such as card systems, which can be a little as a quarter of the price.

Computer security is frequently associated with three core areas as stated:

(a) **Confidentiality**: Ensuring that information is not accessed by unauthorized persons.

(b) **Integrity**: Ensuring that information is not altered by unauthorized persons in away that is detectable by authorized users.

(c) **Authentication**: Ensuring that users are the persons they claim to be.

A strong security protocol addresses all three of these areas. For example, Netscape's SSL (Secure Sockets Layer) protocol, has enabled an explosion in E – commerce which is really about trust (or more precisely, about the lack of trust). SSL overcomes the lack of trust between transacting parties by ensuring confidentiality through encryption, integrity through checksums, and authentication via server certificates. Computer security though not restricted to these three broad concepts, may also include:

a) **Access control:** Ensuring that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive.

b) **Non- repudiation:** Ensuring that the originators of message cannot deny that they in fact sent the messages.

c) **Availability:** Ensuring that a system is operational and functional at a given moment, usually provided through redundancy; loss of availability is often referred to as "denial –of-services"

d) **Privacy**: Ensuring that individuals maintain the right to control what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for.

Form one perspective, the concepts of privacy; confidentiality; and security are quite distinct and possess different attributes. Privacy is a property of individuals; confidentiality is a properly of data; and security is a property assigned to computer hardware and software systems. From a practical perspective, the concept are interwoven. A system that does not maintain data confidentiality or individual privacy could be "secure," but it probably would not be wise to deploy anywhere in the real world. Computer security can also be analyzed by function. It can be broken into five distinct function. It can be broken into five distinct functional areas:

e) **Risk Avoidance:** A security fundamental that starts with questions like: Does my organization or business engaged in activities that are too risky? Do we really need an unrestricted internet connection? Do we really need to computerize that secure business process?

Should we really standardize on a desktop operating system with no access control intrinsic?

f) **Deterrence:** Reduces the threat to information asserts through fear. It can consist of communication strategies designed to impress potential attackers of the likelihood of getting caught.

g) **Prevention:** the traditional core of computer security consists of implementing safeguards.

h) **Detection**: Works best in conjunction with preventative measures. When prevention fails, detection should kick in, preferably while there is still time to prevent damage. Includes log-keeping and auditing activities.

i) **Recovery**: When all else fails, be prepared to pull out backup media and restore from scratch, or cut to backup servers and net connections, or fall back on a disaster recovery facility. Arguably, this function should be attended to before the others.

Analyzing security by function can be a valuable part of the security planning process; a strong security policy will address all five areas, starting with recovery.

Security Domains

Computer security is also frequently defined in terms of several interdependent domains that roughly map to specific departments and job titles.

(a) Physical security: Controlling physical access to system.

(b) Operational/procedural security: Converting everything from managerial policy decisions to reporting hierarchies

(c) Personnel security: Hiring trustworthy employees, background screening, training, security briefings, monitoring, and handling departures.

(d) System security: User access and authentication controls, assignment of privilege, maintaining file and file system integrity, backups, monitoring processes, log-keeping and auditing.

(e) Network security: protecting network and telecommunications equipment, protecting network servers and transmissions, combating eavesdropping, controlling access from untrusted networks, firewalls, and detecting intrusions.

3.9 FIREWALL

Access control on a host means the establishing and maintaining a list of authorized users with their system privileges clearly defined so they can do only hat they are allowed to do. It is fundamental in preventing insider attack and in reducing the damage caused by such an attack or in controlling potential system penetration by an outside hacker masquerading as a legitimate system user.

Firewalls serve a similar purpose at the network level-to control potential damage and to protect the internal network in the event of an internet intrusion. Businesses usually use two types of firewalls: packet filtering and proxy servers.

(a) Packet filtering operates on the principle of "that which is not expressly permitted is denied" to prevent anyone from accessing the network unless they are approved users or are making contact from pre-approved remote sites. Basically, a packet filter checks data packet headers for the data's originating IP address. Only if the IP address is on an approve list is the message passed on. In a filtering firewall from a source to a destination with the router assuming a transparent role.

(b) Proxy server taken an opposite approach. They will stop the connection from the source and initiate a second connection to the destination. The earlier model of proxy.

Servers often referred to as “dual home gateways”, sit between two networks and act as the choke point between them. To establish a connection between the two networks, the user would have to log into the gateway and then establish a connection to the destination. The retrieved information will have to be deposited on the gateway before it can be transported to the user’s individual workstation.

Proxy servers are also equipped with network address translation capabilities. They can hide internal addresses from outsiders. Potential intruders who may capture packets sent through this firewall would see only that firewall’s IP address, not the hundreds or thousands of individual network addresses, which constitute the international network.

Despite its many benefits, firewalls are not panacea for all internet security problems. Firewalls provide no authenticity of the source of the data. Viruses and bogus packets can pass through the firewalls without detection. Firewalls also lack a methodology to support confidentiality.

Use of USB stick, disks, memory sticks and other removable devices

USB flash sticks are carried along by people across the whole spectrum of society. They are the most popular device for data storage and transportation. They are extremely easy to use and can hold up to 16GB worth of data.

- A USB memory stick is a data storage device that is inserted into the USB port of a PC or laptop. USB memory sticks use Nand Flash memory to store data. Once inserted into the UBS Port of a computer, the USB memory stick acts like an external hard drive and data can be read from and written onto it just like any kind of storage device.

- Using a USB Flash drive or memory Stick

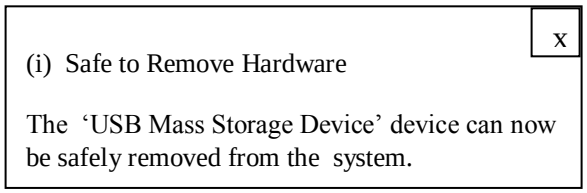
After the USB memory stick has been inserted into the USB Port an icon for another drive should appear in the "my Computer" part of your PC. This will be similar to the icon below.

One can then click on this icon and use it as if it was a hard drive.

Removing your UBS Flash drive or Memory stick

After one has used the USB Memory Flash drive or stick, one will inevitably want to remove it from the computer. Before doing this one makes sure that it is safe to do so, if data is still being transferred between the computer and the memory stick when one is about taking it out, it is likely that one will corrupt the files being transferred. To remove the USB Stick safely, click on the icon with the green arrow in the bottom of the screen.

When you have found the device that you wish to remove select it and click the stop box. The following message should then appear in the bottom right hand side of your screen.



This message tells you that it's safe to remove your memory stick, so you can go ahead and do that.

Protecting Your Memory Stick

Although memory sticks are a very reliable and work even in extreme conditions, it's a good idea to look after your memory stick in order to get the most out of it. Here is some advice on how to protect your memory stick and what's on it.

(a) If you are putting confidential information onto a memory stick, make sure you encrypt it. Memory sticks with confidential information on them have a habit of going astray.

(b) Always remove your USB Memory Stick correctly, following the steps outline above.

(c) Keep you memory stick on you at all times, memory sticks are very easy to steel (a good idea is to put them on your key ring).

(d) Do not expose your memory stick to extreme heat.

(e) Keep your memory stick dry.

SELF ASSESSMENT EXERCISE

* Highlight any five security domains you know.

4.0 CONCLUSION

In this unit, you have learnt about the nature and scope of computer crime and abuse. You have also learnt about the need for security requirement in our network services, the major threats to our information system sources, communication lines and networks. This unit has also introduces you to the usefulness of password etc.

5.0 SUMMARY

Security threats related to computer crime or abuse include – impersonation, Trojan horse method, logic bomb, computer viruses, denial of service, data diddling, Salami technique, spoofing, super zapping etc.

The types of threats to the security of a computer-based information system are best characterized by viewing of the functioning of the computer in providing information. The resources of a computer –based information system can be categorized as hardware, software, data and communication lines as well as networks.

USB flash sticks are the most popular device for data storage and transportation.

6.0 TUTOR MARKED ASSIGNMENT

- In what way is digital watermarks different from digital certificate?

ANSWER TO SELF ASSESSMENT EXERCISE

The following constitute a security Domain:

a. Physical security: Controlling physical access to system.
b. Operating/procedural security
c. Personnel security
d. System security
e. Network security

7.0 REFERENCES/FURTHER READING

Diasey Lucey (2010): Towards Electronic Business, Success Stories and Pitfalls. Prime Wall Publishers, New Jersey.

Yadav D.S. (2008): "Fundamentals of Information Technology, "New Age International Publishers".

James P. Anderson (2000):Computer Security Threats and Surveillance, James P. Anderson & Co.

Ojajuni Jethro (2009): Computer And Business Information System Boomart SCMS Ltd, Lagos.

UNIT TWO

COMPUTER VIRUS, WORMS AND TROJANS, THE THREAT AND PREVENTION

CONTENTS

1.0 INTRODUCTION

The most common blunder people make when the topic of a computer d virus arises is to refer to a worm or Trojan horse as a virus. While the words Trojan, worm and virus are often used interchangeably, they are not exactly the same. Virus, worms and Trojan horses are all malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you to better protect your computer from their often damaging effects.

People continue the spread of a computer virus, mostly unknowingly, by sharing infected files or sending e-mails with viruses as attachments in the e-mail. One the evening of November 2, 1988, the internet was severely compromised by the intrusion of a “worm”. A worm is a

program or a command file that uses a computer network as a means for adversely affecting a systems' integrity, reliability, or availability.

2.0 OBJECTIVE OF THE UNIT

Upon successful completion of this unfamiliar unit, you owe yourself a crucial duty being able to:

- Define and explain what a computer virus is
- Examining the various computer viruses you know.
- Explaining the concept of active x and Java control as a type of computer virus.
- Distinguish between a Trojan horse and computer worm.
- State the prevailing signs of computer infection.
- Explain the relevant preventive measures to computer virus, worms and Trojan horse.
- Identify web trust principles and the criterion for evaluating a site.

3.1 VIRUS, WORMS AND TROJANS, THE THREAT AND PREVENTION

The most common blunder people make when the topic of a computer virus arises is to refer to a worm or Trojan horse as a virus. While the words Trojan, worm and virus are often used interchangeably, they are not exactly the same. Viruses, worms and Trojan horses are al malicious programs that can cause damage to your computer, but there are differences among the three, and knowing those differences can help you to better protect your computer from their often damaging effect.

Computer Virus

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Just as a biological virus spreads by injecting its Deoxyribonucleic Acid (DNA) into a host cell, a computer virus needs to attach itself to a document or program to infect other computers and programs.

Also like a human virus, a computer virus can range in severity: some may cause only mildly annoying effect while others can damage your hardware, software or files.

Almost all viruses are attached to an executable file, which means the virus may exist on you computer but it actually cannot infect your

computer unless you run or open the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going.

People continue the spread of a computer virus, mostly unknowingly, by sharing infected file s or sending e-mails with viruses as attachments in the e-mail.

These viruses are of different categories. Below is a least of the different type of virus that attack the computer system.

3.2 TYPES OF VIRUSES

There are some categories of viruses that can put the computer and all data on it, in danger. These computer viruses include:

3.2.1 Boot Sector Viruses

A boot sector virus infects diskettes and hard drives. All disk and hard drives contain smaller sections called sectors. The first sect is called the boot. The boot carries the Mater Boot Record (MBR). MBR functions to read and load the operating system. So, if a virus infects the boot or MBR of a disk, such as a floppy disk, CDs and DVDs, the hard drive can become infected, if you –re-boot your computer while the infected

disk is in the drive. Once your hard drive is infected. Boot sector viruses often spread to other computers by the use of shared infected disks and pirated software applications. The best way to disinfect your computer of the boot sector virus is by using antivirus software.

3.2.2 Program Viruses

A program virus becomes active when the program file (usually with extensions. BIN, .COM, .EXE, .OVL, .DRV) carrying the virus is opened. Once active, the virus will make copies of itself and will infect other programs on the computer.

3.2.3 Multipartite Viruses

A multipartite virus is a hybrid of a Boot Sector and Program viruses. It infects program files and when the infected program is active it will affect the boot record. So the next time you start up your computer it will infect your local drive and other programs on your computer.

3.2.4 Steal viruses

A stealth virus can disguise itself by using certain tactics to prevent being detected by antivirus software. These tactics include e altering its file size, concealing itself in memory, and so on. This type of virus

is nothing new, in fact, the first computer virus, dubbed Brain, was a stealth virus. A good antivirus should be able to detect a stealth virus lurking on your hard drive by checking the areas the virus infected and evidence in memory.

3.2.5 Polymorphic viruses

A polymorphic virus acts like chameleon, changing its virus signature (also known as binary patter) every time it multiples and infects a new file. By changing binary patterns, a polymorphic virus becomes hard to detect by an antivirus program.

3.2.6 Macro viruses

A macro virus is programmed as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support macro languages. Once a macro virus gets on to your computer, every document you produce will become infected. This type of virus is relatively new and may slip by your antivirus software if you don't have the most recent version installed on your computer.

3.2.7 Active X and Java Control

Some users do not know how to manage and control their web browser to allow or prohibit certain functions to work, such as enabling or disabling sound, pop ups, and so on, leaving your computer in danger of being targeted by unwanted software or hardware floating in cyberspace. Most sites on the web today incorporate features that require special software program to open then – the most common of these are video clips. A computer system that does not have the require software installed on it will be prompted to install a copy of it whenever the user tries to access files that are built on that feature on the web. That copy of the software program will be provided by the web site you are visiting. Hence, this is a very common way of installing virus on you system as in some cases, you will be made to be believe that you are installing a useful software whereas, you are installing a virus onto your system. It is therefore very important to download and install software only from trusted website

3.3 Computer Worm

A worm is similar to a virus by design and is considered to be a sub-class of a virus. Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any human action. A

worm takes advantage of the file or information transport features on your system, which is what allows it to travel unaided.

The biggest danger with a worm is its capability to replicate itself on your system, so rather than your computer sending out a single work, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect. On example would be for a work to send a copy of itself to everyone listed in your e-mail address book. Then, the worm replicates and sends itself out to everyone listed in each of the receiver's address book, and the manifest continues down the line.

Due to the copying nature of a worm and its capability to travel across networks the end result in most cases is that the worm consumes too much system memory (or network bandwidth), causing Web servers, network servers and individual computers to stop responding. In recent worm attacks such as the much –talked –about Blaster Worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

3.4 TROJAN HORSE

The Trojan horse got its name from an incident that occurred in Homer's Iliad. Similar to how the Greeks in Home's poem sent an

army of men, hidden in a wooden horse, to the Trojans to get into the wall of the city.

A Trojan horse is full of as much trickery as the mythological Trojan Horse it was named after. The Trojan horse, at first glance will appear to be useful software but will actually do damage once installed or run on your computer. A Trojan horse appears to be nothing more than an interesting computer program or file. Those on the receiving end of a Trojan horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source. When a Trojan is activated on your computer, the results can vary. Some Trojans are designed to be more annoying than malicious (like changing your desktop, adding silly active desktop icons) or they can cause serious damage by deleting files and destroying information on your system. Trojans are also known to create a backdoor on your computer that gives malicious users access to your system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms. Trojans do not reproduce by infecting other files nor do they self- replicate.

Sometimes, a computer virus is usually hard to detect if it is disguised as a harmless file. In the case of a Trojan horse virus, this type of

virus does not replicate itself like most viruses, but instead opens the computer up to malicious imposters leaving one wondering how it got there. Luckily, the computer after coming in contact with a virus or worm will display some symptoms and signs infection. It is particularly useful to known the signs that indicate an infection. Because one can unintentionally introduce a virus to your computer at anytime one is running an infected program or open an email attachment. To guard against this one needs a good anti- virus program.

3.5 SIGNS OF A COMPUTER INFECTION

Once a computer system is infected with virus some signs that may indicate such include the following:

(a) The computer functions slower than normal;

(b) The computer responds slowly and freezes often;

(c) The computer restarts itself often;

(d) One see uncommon error messages, distorted menus, and dialog boxes;

(e) One notice applications on your computer fail to work correctly and

(f) Printing may not be correctly done.

3.6 PROTECTION AGAINST COMPUTER VIRUSES, WORMS AND TROJANS

While viruses and worms have become common, there are a few ways to avoid these nasty infections. Below is a least of how we can prevent our system from being infected by these nasty element:

(a) You can begin by purchasing a licensed and reliable anti-virus program. This type of software features a scanner equipped with the technology required to detect and eradicate viruses, worms and other members of the malware family. Most importantly you must regularly update the anti-viruses software since virus and worm programs are often written on a daily basis. Make sure that you are using the most up –to-date and enhanced version of your software, so it can catch all those new viruses and worms out there.

Also, make sure to check if you software is installed correctly. Sometimes, people do not install the software properly and realise this only when their computer is attacked with a virus or worm. If you don't know how to install the software, have someone who knows how to, to install it for your. Also, have him or her explain the steps and procedures to you so next time you

need to update or install your software, you can do it yourself. It is also recommended that you purchase an anti- virus program with real-time scanning capability to monitor your incoming emails. This will enable you to scan and attachment to make sure it's safe before opening.

(b) Most of the viruses that spread on the computer are delivered through attachments. These attachment are sent via email most often from people who are unaware of the virus or through spam mail that wants to advertise a message to people.

Email s infected with a virus usually appear like any normal email in your inbox. When the unsuspected user opens the email and the attachment, the virus executes itself and will begin to infect the computer system and other files on the computer and may erase or change information.

If you are not expecting an email or do not recognize the person, then the best idea would be to delete it right away. If you realize later that you do know the person, do not panic. Chances are there that they will write back to you again. Also, be aware of attachments and emails you receive from your own family and

friends. Most of the time, people receive viruses and worms from individuals they know. Your friends may not realized that they are sending you a virus. So, your job is to inform them and fix the problems before it causes more damage.

Finally, when you use email programs, use the ones that have built in spam filters, for instance, Outlook Express, Windows Hotmails and so on. This way, not only will the email be tracked and filtered for viruses, but you will also feel secure that your computer is free from worms and viruses.

(c) Another solid option is a firewall. These components often come as features of anti-virus software or as stand-alone applications. A firewall application will keep unauthorized users from accessing your system and secretly installing malicious content. By implementing these two security solutions, you can stay one step ahead of the busy coders scripting viruses and worms.

3.7.0 WE TRUST

Some of the benefits, when we examine E-commerce that users may derive, include:

(a) Performing transaction with customer over the internet.

(b) Gathering information relating to consumer market research and computers.

(c) Developing information to prospective customers through interactive advertising, sales and marketing efforts.

However, Electronic Commerce is faceless. Crooks, fraudsters and all others in this category can easily get away by designing aesthetic and attractive looking website.

There is the issue of information privacy. Can one be comfortable giving out the credit card number that may be needed to furnish the seller of goods to be bought?

However is one sure that information about the customer will not on way or the other be tempered with either in transit or when it gets to the destination? There is need to assure customers of their transactions, owing to the fears and concern web they have. Web trust is actually a seal of assurance which would be put up on the site to ensure the customers that the people behind the show are genuine, their intentions are honourable, their business policies are unquestionable, their information privacy methods and security techniques are fool proof. In short, they are totally safe to deal with.

Trust on the internet, in particular concerns relating to the protection of personal information, and knowing who you are doing business with as well as their business practices, will surely become a key barrier to the further growth of electronic commerce.

And as consumers become more aware of these issues, there will be an increasing demand for on-line merchants to demonstrate their adherence to good business practices.

Owing to fears and concerns of customers, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants, (CICA) have jointly developed Web Trust, a comprehensive e-commerce assurance service that provides businesses with e-commerce 'best practice' designed to build trust and confidence in this new electronic market place.

Web Trust provides e-commerce 'best practice' that covers:

(a) Security
(b) Confidentiality
(c) Availability
(d) Business practices/transaction integrity
(e) Non –repudiation ; and

(f) Certification authorities, CAS

Web Trust provides a unique combination of a comprehensive standard and an independent audit assurance by specially trained and licensed Certified Public Accountant, Certified Public Accountants CPAs to ensure that an on-line business complies with e-commerce best practice. The CPA firm tests the Web Site, regularly and at least every 6 months to verify that it continues to comply with the Web Trust principles and criteria.

CPAs and CAS are in the business of providing assurance services, the most publicly recognized of which is the audit of financial statements. An audit opinion signed by a CPA or CA is valued because these professionals are experienced in assurance matters and financial accounting subject matter and are recognized for their independence, integrity, discretion, and objectivity. CPAs and CA s also follow comprehensive ethics rules and professional standards in providing their services.

The business and professional experience, subject matter expertise (e-commerce information systems security, auditability, and control) and professional characteristics (independence, integrity, and objectivity) needed for such projects are the same key elements that enable a CPA

or CA to comprehensively and objectively assess the risks, controls, and business disclosures associated with e-commerce.

3.7.1 Web Trust Principles and criterion for Evaluating a Site

There are three broad principles for evaluating a site:

(a) Business and information privacy practices

(b) Transaction integrity

(c) Information protection.

Each of this principle is then divided into several criteria. Each criterion in turn is assessed on the basis of the type of site i.e. whether it is pure information based site, or conducts e-commerce as well, or is involved in online banking transactions, or also in online securities trading. The site owner must furnish relevant information, i.e. disclose business practice in all of these columns which are applicable to him. The entity must be in conformity with these criteria to obtain and maintain its Web Trust Seal.

The entity must be able to demonstrate over a period of time (at least two months) that:

(a) It executed transactions in accordance with the business practices it discloses for e-commerce transactions;

(b) It controls operations effectively;

(c) It maintains a control environment that is conducive to reliable business practice disclosures and effective controls; and

(d) It maintains monitoring procedures to ensure that such business practices remain current and such controls remain effective in conformity with the Web Trust Criteria.

These concepts are integral parts of the Web Trust Criteria.

3.7.2 WEB TRUST SEAL

The Web Trust Seal of assurance is a symbolic representation of a practitioner's unqualified report. It also indicates to customers that they need to click to see the practitioner's report. This seal can be displayed on the entity's Web site together with links to the practitioners report and other relevant information.

Already a lot of web sites have obtained this seal of assurance and a lot many are in the process.

For customers it will be situation of faith and confidence. For the genuine businessmen, it will easily give them the respect and immediate recognition and this will naturally help them grow. And finally for e-commerce it will be growth, prosperity and more growth. A win-win situation.

SELF ASSESSMENT EXERCISE

- Differentiate between program viruses and multipartite viruses.

4.0 CONCLUSION

This unit being as comprehensive as it is has let you know and discover so much in information and communication technology (CIT 301). You have another opportunity offered you to learn about a computer virus, internal worm and Trojan horses. You have also learnt about the various types of computer viruses and the relevant preventive measures to be put in place.

5.0 SUMMARY

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, viruses encompass – boot sector

viruses, program viruses, multipartite viruses, polymorphic viruses and others. A worm is similar to a virus by design and is considered to be a subclass of a virus. Worm spread from computer to computer, but unlike a virus.

In recent worm attacks such as the much talked –about Blaster worm, the worm has been designed to tunnel into your system and allow malicious users to control your computer remotely.

6.0 TUTOR MARKED ASSIGNMENT

Critically discuss web trust principles and the criterion for evaluating a site.

Answer To Self Assessment Exercise

A program virus becomes active when the program file (usually with extensions BIN,.Com, .EXE, .OVL, .DRV) carrying the virus is opened. Once active, the virus will make copies of itself and will affect other programs on the computer.

While a multipartite viruses is a hybrid of a Boot sector and program viruses. It infects program files and when the infected program is active it will affect the boot record.

7.0 REFERENCES/FURTHER READING

Graham Curtis (2001): Business Information System Analyst, Design and Practice; 3rd Edition, Addision Wesly.

James P. Anderson (200): "Computer Security Threats and Surveillance; James P. Anderson and Co.

Y. Koyeyinka and Ayeni (2006): Introduction to Management Information Systems: 2nd Edition Famorks Publishers, Lagos.

UNIT THREE

INFORMATION SYSTEMS ARCHITECTURE (COMMUNICATION NETWORKS)

CONTENTS

3.3.6 Remote system

3.4 Distributed systems, mobile facilities

3.4.1 Goals and advantages

3.4.2 Drawbacks and disadvantages

3.5 Hardware (Main frame, Server, outer, workstation)

3.6 Software systems (systems software, application software, utility programs)

3.6.1 Operating systems

3.6.2 Utility software

3.7 Application development environment (ADE)

3.8 Data organization or access methods

3.8.1 Files, tables, databases and data based management.

3.9 Protocol Standards and enabling technologies

3.9.1 Professional accountants and career in it path

4.0 Conclusion

5.0 Summary

6.0 Tutor marked assignment

7.0 References/further reading

1.0 INTRODUCTION

Communication networks provide essential services like most other ubiquitous utilities such as the power and water supply system. Communication networks are quite flexible in their uses and in this respect manifest similar characteristics with the transportation networks and both have become essential infrastructure of every society.

Local area network (LAN),Metropolitan Area network (MAN) and wide area networks (WAN), metropolitan area networks (MAN) and wide area networks (WANT) constitute the three major types of networks we have.

The main goal of a distributed computing system is to connect users and resources in a transparent, open, and scalable way. Software is an ordered sequence of instructions for changing the state of the computer hardware in a particular sequence. Here, the operating system acts as a host for applications that are run on the machine. Utility software has long been integrated into most operating systems.

An application development environment normally consists of a: source code editor, compiler and/or interpreter, build automation tools and debugger.

2.0 OBJECTIVES OF THE UNIT

At the end of this unit, you should be able to:

- Define and explain communication networks
- Examine the various components of communication networks
- Identify and discuss the types of networks we have
- Distinguish between a client networks and remote system.
- Ascertain the goals and drawbacks of distributed systems, mobile facilities.
- Identify the nexus between operating system and utility software
- Explain the concepts and advantages of data based management system.

3.1 COMMUNICATION; DEFINITION AND MEANING

A communications network in its simplest form is a set of equipment and facilities that share common communication media such as

cables, modem, etc in order to provide a service or services. The most common example of communication network is the telephone network providing telephone service which is the bidirectional transfer of voice signals between two people exchanging information. Other examples include:

(a) the computer network

(b) television broadcast network

(c) mobile phone networks and

(d) the internet

Communication networks provides essential service like most other ubiquitous utilities such as the power and water supply system. Communication networks are quite flexible in their use and in this respect manifest similar characteristic with the transportation network and both have become essential infrastructure of every society. Communication networks are enabled by complex and flexible connectivity that facilitate the transmission of data, signals or information. This chapter shall dwell on the communication networks as deployed in information transmission and management.

3.2 COMMUNICATION NETWORK COMPONENTS

All communication networks are made up of five basic components that are present in each network environment regardless of type or use. These basic components include terminals, communications processors, communications channels, computers, and communication control software.

3.2.1 Terminal

Terminals are the staring and stopping points in any communication network environment. Any input or output device that is used to transmit or receive data can be classified as a terminal component.

3.2.2 Communication processor

Communication processors are used to support data transmission and reception between terminals and computers by providing a variety of control and support functions. (i.e. convert data from digital to analog and back).

3.2.3 Communication channels

Communications channels are the way in which data is transmitted and received. Communication channels are created through a variety of different media. The most popular methods are found in the home

which includes copper wires, and coaxial cables. More and more frequently fiber-optic cables are being used to bring faster and more robust connections to businesses and homes.

3.2.4 Computers

In a communication environment computers are connected through some form of communication media to perform their communication assignments.

3.2.5 Communications control software

Communication control software is present on all computers and are responsible for controlling network activities and functionality.

3.3 TYPES AND CLASSIFICATION OF NETWORK

There are three major types of networks which are wide area networks (WAN), Metropolitan Area network, (MAN) and local areas networks (LAN). The other types are various applications of these three to satisfy organisation's information systems architecture requirements. These type of networks include client/server networks and network computing.

3.3.1 Local Area Network

A local area network (LAN) is a network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport. The defining characteristics of LANs, in contrast to wide-area networks (WANs), include their usually higher data-transfer rates, smaller geographic place, and lack of a need for leased communication lines.

The development and proliferation of personal computers from the late 1980s and then DOS-based personal computers from 1981 meant that a single site began to have dozens or even hundreds of computers. The initial attraction of networking these was generally to share disk space and laser printers, which were both very expensive at the time. This was what gave rise to the initial computer network that eventually developed into what obtains today.

3.3.2 Metropolitan Area Network

A metropolitan area network (MAN) is a large computer network that spans a metropolitan area. Its geographic scope falls between a WAN and LAN. MAN provides internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the

internet. A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate –to-high data rates. A MAN might be owned and operated by a single organizations. MANs might also be owned and operated as public utilities. They will often provide means for internetworking of local network. Metropolitan area networks can span up to 50km, devices used include modem and wire/cable.

3.3.3 Wide Area Network (Wan)

This is a communications network that covers a broad area (i.e. any network whose communications links cross metropolitan regional, or national boundaries). The largest and most well-known example of a WAN is the Internet. WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computer in other locations. Many WANs are built for one particular organization and are private. Others, built by internet services providers, provide connect from an organization's LAN to the Internet.

3.3.4 Client/Server network

In a client/server environment the client (i.e. PC) relies on a LAN to connect with a back office network server that is responsible for the connection, retrieval, and storage or data and other critical company or personal information. The client/server network architecture continues to be the main architectural choice for most enterprise network computing.

3.3.5 Network computing

Network computer is a network architecture that has rapidly picked up steam with the growth of the internet and resulting connection speeds. In a network computing architecture a computer uses it web browser to connect to another network computer that actually is running the application. A good example of this architecture in use if Google Docs, or Microsoft Office online. Both services allow users the ability to login to Google or Microsoft servers respectively and work similarly to how it would be performed in their own computing environment.

3.3.6 Remote system

Remote system refers to the accessing and controlling a computer from a remote location. Software that allows remote administration is becoming increasingly common and is often used when it is difficult or

impractical to be physically near a system in order to use it, or in order to access web material that is not available in one's location. A remote location may refer to a computer in the next room or one on the other side of the world. It may also refer to both legal and illegal (i.e. hacking) remote administration.

Wireless Remote Administration

Remote system also includes wireless devices such as the BlackBerry, Pocket PC, and Palm devices, as well as some mobile phones. Generally, these solutions allow administrators and users to keep in touch with the office while on the move.

3.4 DISTRIBUTED SYSTEMS, MOBILE FACILITIES

A distributed system is an information system consisting of hardware and software systems that involve more than one processing element or storage element, concurrent processes, or multiple programs, running under a loosely or tightly controlled regime. In distributed system, a program is split up into parts that run simultaneously on multiple computers communicating over a network. Distributed computing requires dividing a program into parts that can run simultaneously, dealing with heterogeneous computing environments,

network links of varying latencies, and unpredictable failures in the network or the computers.

3.4.1 Goals and advantages

There are many different types of distributed computing systems and many challenges to overcome in successfully designing one. The main goal of a distributed computing system is to connect users and resources in a transparent, open and scalable way. Ideally, this arrangement is drastically more fault tolerant and more powerful than many combinations of strand-alone computer systems. Openness is the property of distributed systems such that each subsystem is continually open to interaction with other systems.

3.4.2 Drawbacks and disadvantages

If not planned properly, a distributed system can decrease the overall reliability of an information system as the unavailability of a node can cause disruption of the other nodes. In a distributed system, the failure of a computer a user odes not known existed can render his own computer unusable. Troubleshooting and diagnosing problems in a distributed system can also become more difficult, because the

analysis may require connecting to remote nodes or inspecting communication between nodes.

Many types of information systems application are not well suited for distributed environments, typically owing to the amount of network communication or synchronization that would be required between different users. If the communication requirements are substantial, then the benefits of distributed computing may be negated and the performance may be worse than a non-distributed environment.

3.5 HARDWARE (MAINFRAME, SERVER, ROUTER, WORKSTATION

Different types of hardware devices are involved in communications network. Some of these are discussed below:

Mainframe: A mainframe computer is a high-level computer designed for the most intensive computational tasks. Mainframe computers are often shared by multiple users connected to the computers via terminals. The most powerful mainframes, called supercomputers, perform highly complex and time-consuming computations and are used heavily in both pure and applied research by scientists , large business, and the military. Modern mainframe computers are mostly

used as web servers containing high capacity storage media, large computer memory and speed so as to meet the challenges of internet information requests.

Router: A router is a networking devices whose software and hardware are usually tailored to the tasks of routing and forwarding information. For example, on the internet, information is directed to various paths by routers.

Server: A server is computer that provides services used by other computers. For example a web server is a computer hosting a web site and serves up web pages. A server is a computer that has been set aside to run a specific server application. Server is also used as a designation for computer models intended for use in running server applications under heavy workloads, also called operating units often unattended and for an extended period of time. While any workstation computer is capable of acting as a server, a serve computer usually has special features intended to make it more suitable. These features can include a faster CPU, faster and bigger RAM, and larger storage media e.g. hard drives.

Workstations: A workstation is a microcomputer designed and intended primarily to be used by one person at a time. They are commonly

connected to a local area network and run multi-user operating systems. The term workstation has also been used to refer to a mainframe computer terminal or a PC connected to a network.

Historically, workstations had offered higher performance than personal computers, especially with respect to CPU and graphics, memory capacity and multitasking capability. They are optimized for the visualization and manipulation of different types of complex data such as 3D mechanical design, engineering simulation (e.g. computational fluid dynamics), animation and rendering of images, and mathematical plots. They are usually made up of a high resolution display, a keyboard and a mouse at a minimum, but also offer multiple displays, graphics tablets, 3D mice (devices for manipulating and navigating 3D objects and scenes), etc.

3.6 Software systems (systems software, application software, utilities programs

Computer software is a collection of computer programs and procedures that perform different tasks on a computer system. Computer software are often regarded as anything but hardware, meaning that the 'hard' are the parts that are tangible while the 'soft' part is the intangible object inside the computer. Software

encompasses an extremely wide array of products and technologies developed using different techniques like programming languages, scripting languages or even microcode.

Software is an ordered sequence of instructions for changing the state of the computer hardware in a particular sequence. At the lowest level, software consists of a machine language specific to an individual computer processor. A machine language consists of groups of binary values signifying processor instructions which change the state of the computer from one state to another when performing a tasks or a set of tasks. At a higher level, software is usually written in high-level languages are compiled or interpreted into machine language object code.

Practical computer systems divide software systems into two major classes: System software and application software. System software included operating systems and utility software and utility software. These are explained below:

System software is software that basically makes the computer work. It is the computer software that provides the infrastructure over which programs can operate, i.e. it manages and controls computer hardware so that application software can perform. Operating

systems, such as GNU, Microsoft Windors, Mac, OS X or Linux, are prominent examples of system software. Besides operating systems, other examples are device driver software and utility software. Without the system software the computer doesn't work. System software perform tasks like transferring data from memory to disk, or rendering text onto a display device.

3.6.1 Operating systems

An operating system (commonly abbreviated to either OS or O/S) is an interface between computer hardware and user; it is responsible for the management and coordination of activities and the sharing of the limited resources of the computer. The operating system acts as a host for applications that are run on the machine. As a host, one of the purposes of an operating system is to handle the details of the operating of the hardware. This relieves application programs from having to manage these details and makes it easier to write applications. Almost all computers, including handled computers, desktop computers, supercomputers, and even video game consoles , use an operating system of some type. Some of the oldest models may however use an embedded operating system, that may be contained on a compact disk or other data storage device. Common contemporary

operating systems including Microsoft windows, Mac OS, Linux, and Solaris. Microsoft windows has a significant majority of market share in the desktop and notebook computer markets, while servers generally run on Unix or Unix-like systems. Embedded device markets are split amongst several operating systems.

3.6.2 Utility Software

Utility software (also known as service program, service routine, tools, or utility routine) is computer software designed to help manage and tune the computer hardware, operating system or application software by performing a single tasks or a small range of tasks. Utility software has long been integrated into most major operating systems.

Examples

Disk storage utilities

(a) Disk defragmenters can detect computer files whose contents are stored on the hard disk in disjointed fragments, and move the fragments together to increase efficiency.

(b) Disk checkers can scan the contents of a hard disk to find filers or areas that are corrupted in some way, or were not

correctly saved, and eliminated them for a more efficiently operating hard disk.

(c) Disk cleaners can find files that are unnecessary for computer operation, or take up considerable amounts of storage space. Disk cleaner helps the user to decide what to delete when their hard disk is full.

(d) Disk partitioners can divided an individual disk into multiple logical disk, each with its own files storage system which can be identified by the operating system and treated as an individual storage medium disk.

(e) Backup utilities can help users make a copy of all information stored on a disk, and restore either the entire disk (e.g. in an event of disk failure) or selected files (e.g. in an event of accidental deletion).

(f) Disk compression utilities can transparently compress/uncompress the contents of a disk to increase the capacity of the disk.

(g) File managers provide a convenient method of performing routine data management tasks, such as deleting , renaming,

cataloging, uncataloging, moving, copying, merging, generating and modifying computers files.

(h) System profilers provide detailed information about the software installed and hardware attached to the computer.

(i) Anti-virus utilities scans, detects and removes computer viruses.

(j) Data compression utilities output a shorter stream or a smaller file when provided with a stream or file.

(k) Cryptographic utilities encrypt and decrypt streams and files.

(l) Launcher applications provide a convenient access point for application software.

(m) Registry cleaners clean and optimize the windows registry by removing old registry keys that are no longer in use.

(n) Network managers check the computer's network, log events and check data transfer.

Application software

In contrast to system software, application software are designed to drive specific business processes such as creating text documents, financial reporting processing, banking operations, or other routine

office activities that were hitherto performed manually. In general application software are programs that enable the end –user to perform specific, productive tasks, such as word processing or image manipulation, etc.

3.7 APPLICATION DEVELOPMENT ENVIRONMENT (ADE)

Application Development Environment or what is also being referred to as an integrated development environment (IDE) also known as integrated design environment is a software application that provides comprehensive facilities to computer programmers for software development. ADEs typically present a single program in which all development is done. This program typically provides many features for authority. Modifying, compiling, deploying and debugging software. An application development environment normally consists of a:

(a) Source code editor;

(b) Compiler and/or interpreter

(c) Build automation tools; and

(d) Debugger.

Sometimes a version control system and various tools are integrated to simplify the construction of a GUI. Many modern IDEs also have a

class browser, an object inspector, and a class hierarchy diagram, for use with object-oriented software development.

ADEs (or IDEs) are designed to maximize programmer productivity by providing tightly-nit components with similar user interfaces. This means that the programmer has much less to do switching in between modes to have access to needed programming facilities especially when using discrete development programs. However, because an ADE is by its very nature a complicated piece of software, this high productivity only occurs after a lengthy learning curve.

Typically an IDE is dedicated to a specific programming language, so as to provide a features set which most closely matches the programming paragidms of the language. However, some multiple-language IDEs are in use, such as Eclipse, Active State Komodo, recent versions of NetBeans, Microsoft Visual Studio and WinDev.

3.8 DATA ORGANIZATION OR ACCESS METHOD

Computer systems store files on secondary storage devices. Records can be arranged in several ways on storage media, and the arrangement determines the manner in which individual records can be access or retrieved.

Sequential file organization: Data can be retrieved in the same sequence in which they are stored. Sequential file organization is the only file organization that can be used on magnetic tape.

Direct/Random file organization: Data can be retrieved in any desired sequences without regard to the actual physical order on the storage media. Direct file access method is used with direct file organization. The method uses a key field to locate the physical address of a record. However, this is done by using a mathematical formula called a transform algorithm to translate the key field directly into the records' physical storage location on disk.

Indexed sequential access method: A file access method to directly access records organized sequentially using an indexed of keys fields. An index to a file is a table or list that relates record keys to physical locations on direct access files.

3.8.1 Files, Tables, Database & Data Base Management Files

A computer system organizes data in a hierarchy that starts with bits and bytes and progresses to fields, records, files, and database (see).

a. Database

A group of related files/tables make up a database. The student course file illustrated in figure 3.1.9 could be grouped with files on student's personal histories and financial background s to create a student database. In business terms, a record describes an entity. An entity is person, place, thing or event on which we maintain information. An order is a typical entity in a sales order file, which maintains information on a firm's sales order. Each characteristics to as field. For example, order amount, item number, and item quantity would each be an attribute of the entity order.

Every record in a file should contain at least one field that uniquely identifies that records so that the record can be retrieved, updated, or sorted. This identifies field is called a key field. An example of a key field s is the order number of the order record, or an employee number for a personnel record (containing employee data such as the employee's name, age, address, job title, and so forth).

b. Database management system

A database management system (DBMS) is simply the software that permits an organization to centralize data, manage then efficiently, and provide access to the stored data by application programs. DBMS acts as an interface between application programs and the physical data

files. When the application program calls for a data items such as gross pay, the DBMS finds this item in the database and present it to the application program. Using traditional data files the programmer would have to define the data and then tell the computer where they are. A DBMS eliminates most of the data definition statements found in traditional programs.

A database management system has three components:

(a) A data definition language

(b) A data manipulation language

(c) A data dictionary

The data definition language is the formal languages used by programmers to specify the content and structure of the database. The data definition language defines each data element as it appear in the database before that data element is translated into the forms required by application programs.

Examples:

CREATE TABLE salesman (SalesID c(6) PRIMARY KEY, SaleName C(20))

CREATE TABLE customer, (SalesID c(6), Custidi PRIMARY KEY,

CustName c(20) UNIQUE, SalesBranch c(3)

The first example says create a table called salesman with sales id of six characters as the primary key and sale name of 20 characters.

Most DBMS have a specialized language called a data manipulation language that is used in conjunction with some conventional third – or fourth – generation programming languages to manipulate the data in the database. This language contains commands that permit end users and programming specialists to extract data from the database to satisfy information request and develop applications. The most prominent data manipulation language today is Structured Query Language, or SQL.

Examples:

SELECT * FROM salesman

Select fname,lname,empID, doBirth from employees where emID = 34554.

The third element of a DBMS is a data dictionary. This is an automated or manual file that stores definitions of data elements and data characteristics such as usage, physical representation, ownership (who in the organization is responsible for maintaining the data), authorization, and security. Many data dictionaries can produce lists and reports of data utilization, groupings, program locations and so on. By creating an inventory of the pieces of data contained in the database, the data dictionary serves as an important data management tool. For instance, business users could consult the dictionary to find out exactly what pieces of data re maintained for the sales or marketing function or even to determine all the information maintained by the entire enterprise. The dictionary could supply business users with the name, format, and specifications required to access data for reports. Technical staff could use the dictionary of determine what data elements and files must be changed if a program is changed.

Advantages of Database Management Systems

(a) Complexity of the organizations' information system environment can be reduced by central management of data, access, utilization, and security.

(b) Data redundancy and inconsistency can be reduced by eliminating all isolated files in which the same data elements are repeated.

(c) Data mix-up can be eliminated by providing central control of data creation and definitions.

(d) Program-data dependence can be reduced by separating the logical view of data from its physical arrangement.

(e) Program development and maintenance costs can be radically reduced.

(f) Flexibility of information systems can be greatly enhanced by permitting rapid and inexpensive ad hoc queries of very large pools of information.

(g) Access and availability of information can be increased.

3.9 PROTOCOLS, STANDARD AND ENABLING TECHNOLOGIES

In computing, a protocol is a convention or standard that controls or enables the connection, communication, and data transfer between computing endpoints. In its simplest form, a protocol can be defined as

the rules governing communications over a network. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behaviour of a hardware connection.

A. Typical properties of protocols

While protocols can vary greatly in purpose and sophistication, most specify one or more of the following properties.

a) Detection of the underlying physical connection (wired or wireless), or the existence of the other endpoints.

b) How to start and end a message.

c) How to format a message

d) What to do with corrupted or improperly formatted messages (error correction).

e) How to detect unexpected loss of the connection, and what to do next.

f) Termination of the session and or connection.

B. Common protocols

Common protocols used for today's data communications include:

IP (Internet Protocol): The Internet protocol (IP) is a protocol used for communicating data across a packet-switched internet work using the internet protocol suite, also referred to as TCP/IP/IP is the primary protocol in the internet layer of the internet protocol suit and has the tasks of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

TCP (Transmission Control Protocol): Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the internet, TCP operates at a higher level, concerned only with the two end systems, for example a Web browser and a Web server. In particular, TCP provides reliable, ordered delivery of a stream of bytes from one program on one computer to another program on another computer.

UDP (User Datagram Protocol): The user datagram protocol (UDP) is one of the core members of the internet protocol suite, the set of network protocols used for the internet. With UDP, computer applications can send messages referred to as datagrams, to other computers on an internet protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP is sometimes called the universal datagram protocol.

HTTP (Hypertext Transfer protocol): This is an application –level protocol for distributed, collaborative, hypermedia information systems. Its use for retrieving inter-linked resources led to the establishment of the world web. HTTP is a request/response standard of a client and a server.

FTP (File Transfer protocol): Is a network protocol used to exchange and manipulate files over a TCP computer network, such as the internet. An FTP client may connect to an FTP server to have access to and manipulated files on that server as if the files are directly on the local storage medium.

POP3 (Post Office Protocol): The Post Office Protocol version 3 (POP3) is an application –layer internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

SMTP (Simple Mail Transfer protocol): Is an Internet standard for electronic mail (e-mail) transmission across internet protocol (IP) networks.

IMAP (Internet Message Access Protocol): The IMAP is a standard protocol s for e-mail retrieval.

SOAP (Simple Object Access Protocol): SOAP, is a protocol specificiatin for exchanging structure information in the implementation of Web Services in computer networks. It is relies on extensible Markpu Language (XML) as its message format, and usually relies on other application layer protocols (most notably remote procedure call (RPC) and HTTP) for message negotiation and transmission.

3.9.1 Professional Accountants and Career Paths in IT

Under the IFAC practice statement no. 2 issued in 2008, and recommending detailed IT knowledge and skill required of a chartered accountant, a professional accountant qualifying under that curriculum and indeed the present ICAN curriculum will have a broad range of choices in the IT career line. These include but not limited to:

(a) Information system manager

(b) Computer analyst

(c) Application software designer

(d) IT consultant in the areas of software deployment and implementation;

(e) Information systems security manager

(f) Information systems auditor

(g) Computer hacking professional; and

(h) Computer hacking and forensic investigation, etc.

SELF ASSESSMENT EXERCISE

- What is integrated development environment?

4.0 CONCLUSION

This unit is considered reach in the sense that it has broadened your mind in the area of communication, and information networks. You have learnt about the various components of communication network, types and classification of networks, distributed systems mobile facilities and the operating systems. You have also learnt about the application development environment and data organization or access methods.

5.0 SUMMARY

A communication network in its simplest form is a set of equipment and facilities that share common communication media such as cables, modem, etc in order to provide a service or services. Networks are classified into – local area network, metropolitan area net work and wide area network and server/client network. In a distributed system, a

program is split up into parts that run simultaneously on multiple computers communicating over a network.

Mainframe computer is a high level computer designed for the most intensive computational tasks. A computer system organizes data in a hierarchy that starts with bits and bytes and progress to fields, records, files, and data bases.

6.0 TUTOR MARKED ASSIGNMENT

- Discuss succinctly the advantages of database management systems.

Answer to Self Assessment Exercise

The term integrated development environment is also known as application development environment. It is a software application that provides comprehensive facilities to computer programmes for software development. It normally consists of source code editor, computer and/or interpreter, build automation tools and debugger.

7.0 REFERENCE/ FURTHER READING

Dan Farmer and Wiester Venema (2002): 'Forensic Computer Analysis. an Introduction, "Techweb.

Charles T. Betz (2007): "A Guide To Conceptual Data Models for It Managers: Prentice Hall New York.

Charles Parker (2008): Management Information Systems, Strategy and Action," McGraw-Hill Publishers.

Daniel Saber, (2001): "Privacy Issues in Computer Medicated Communications".

UNIT FOUR

SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

CONTENT

1.0 INTRODUCTION

The system life cycle is the series of stage involved in replacing (especially manual) an old system by a new one (computerized). Unlike the life cycle of an insect, which follow universally agreed stages. System life cycle lacks such a universal agreement, because the ultimate life cycle of a system depends very much on the system itself. However, the following stages are the possibly recognized –preliminary, project planning, feasibility study, investigation and fact finding, analysis, design, implementing, maintenance and review.

When arrange in order from beginning to the end, the whole discipline of system analysis resolves around the system life cycle. The preliminary survey is something of a small-scale feasibility study. It is aimed at ascertaining the aims and objectives of a new system, should one be required. The feasibility study aims at determining the technical, social and economical feasibility of the system. The investigation fact finding stage is out to know all the weakness and strengths the old system in order to eliminate the weakness and retain the strengths.

2.0 OBJECTIVE OF THE UNIT

At the end of this unit, you are expected to do the following:

- Define and explain system development life cycle (SDLC).
- Examine the nature of investigation and feasibility study
- Discuss the scope of feasibility study involving formation of the steering committee, setting up the terms of reference, formation of the studying group and planning the study and problem definition as well as information gathering.
- Undertake a thorough assessment of the feasibility study to include technical feasibility, operational feasibility, social, economic, and financial justification of the feasibility study.
- Explain the concept of project identification and approval.

3.1 SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

Systems development life cycle (SDLC), or software development life cycle refers to the process of developing a new or amending existing information systems, and the methodologies employed to develop these systems. It is a formalized process of building information systems in a very deliberate, structured and methodical way, reiterating each stage of the life cycle.

An SDL should result in a high quality system that meets or exceeds customer expectations, reaches completion within time and cost estimate, works effectively and efficiently in the currently in the current and planned information technology infrastructure, and is inexpensive to maintain and cost –effective to enhance.

Systems acquisition/development phases and tasks:

The stages in system development.

3.2 INVESTIGATION AND FEASIBILITY STUDY

The need for an information system is usually identified when a problem arises in the day-to-day business operations of an organization. The first step in project definition is therefore to identify what the problems is, explore the possibility of a system solution and undertake a feasibility study.

A feasibility study is a formal study to decide what type of system can be developed that meets the needs of the organization and the user objectives. It is a preliminary study that investigates the information needs of end users and the objectives, constraints, basic resource requirements, cost/benefits, and feasibility of proposed projects.

Broadly, it considers whether a proposed system can be implemented to meet the information requirements. It reveals possible solutions to the problem that has been identified and considers if the cost of developing a new system is justified.

It involves a limited investigation and analysis of the problem and the alternatives to the current system so that management can take a decision as to whether or not commit resources, time, hardware and expertise to the project. This is a stage in the systems life cycle that analyses the problems of existing systems, define the objectives to be attained by a solution, and evaluates various solution alternatives for management consideration. Feasibility study defines the business case, identifies the strategic benefits of the new system and provides justification for proceeding with the project. Some of the work completed during the feasibility study may be used at the investigation, analysis and design stages.

Feasibility study attempt to provide answers to questions such as:

a) What do the existing system do?
b) What are their strengths, weakness and problems?

c) What should a new or modified system do to solve these problems?

d) What users information requirements must be met by the solution?

e) What alternative solution options are feasible?

f) What are their costs and benefits?

3.3 SCOPE OF FEASIBILITY STUDY

Within the feasibility study, the following are addressed:

a) Defining the time and scope for the implementation of the required solution.

b) Establishing optimum solution for meeting business needs and general information resource requirements.

c) Finding out if an existing system can correct the situation with or without modifications or a new system is required.

d) Identifying IT products that offer solutions to the problems.

e) Estimating the cost to develop the system

f) Agreeing on how well the proposed solution fits the business strategy.

a. Feasibility study stages

The feasibility study can be split into the following stages:

(a) Formation of the steering committee

(b) Setting up the terms of reference

(c) Formation of the study group

(d) Planning the study

(e) Problem definition and information gathering

(f) Assessing feasibility

(g) Project identification

(h) Feasibility study report; and

(i) Giving go-ahead for the system project.

3.3.1 Formation of the steering committee

If an organizational steering committee does not exist, then a specific steering committee will be set up. The steering committee, must relate

the feasibility study proposed to the original project objectives. If these objective are met, and the project proposal is approved, then the more specific details in the proposal should be considered and approved.

A steering committee is a group of members from various departments within the organization and is not, therefore, biased towards one particular functional area of the business. The purpose of a steering committee is to decide how to allocate IT resources and to plan for the future system development.

Other activities of the Steering committee include:

(a) Ensuring that all the information technology activities are in line with the strategic plans of the organization as a whole;

(b) Providing leadership at senior level for the utilization and management of information technology;

(c) Ensuring that resources allocation decisions are effective;

(d) Coordinating requirements in any organization restructuring;

(e) Creating the terms of reference for the project teams; and

(f) Monitoring the progress of the various projects.

3.3.2 Setting up the terms of reference

The initial tasks in system investigation must be to establish terms of reference for the design team. The decision to change the information system may have derived from one or several causes, such as inaccurate information, the need to have a more integrated system combining the information requirements of all management, or the need for quicker or simply, more complete information. Terms of reference establish what the systems team is expected to achieve as a result of the changes they make, and will establish a timetable for the planning and implementation of these changes.

3.3.3 Formation of the study group

The steering committee may appoint a systems analyst, or hire one from an outside consultancy who will then approach people who posses the requisite abilities and experience.

The feasibility team is responsible for the detailed work in the feasibility study. There are a number of important points to consider in connection with the members of the group:

(a) One person should not attempt to carryout the feasibility study on his own;

(b) Some members of the team should; where possible, be drawn from the departments affected by the project;

(c) At least one person must have in-depth knowledge of computers and system design (in a small organization, it is usually necessary to bring in a systems analyst from outside);

(d) At least one person should have a detailed knowledge of the organization and in particular of the operations and staff of the departments affected.

(e) It is possible to hire consultants to carry out the feasibility study, but their lack of knowledge about the organization may adversely affect the usefulness of their proposals;

(f) Before selecting the members of the study group, the steering committee must ensure that they possess suitable personal qualities, for example, the ability to be objectively critical;

(g) All members of the study group should undergo some form of training in systems design. They should also be encouraged to read as widely as possible and take an active interest in current innovations.

(h) Ideally, the study group should be directly responsible to the steering committee and not incorporated into one of the normal functional departments.

(i) Provisions for redeployment of members of the group after the completion of the study should be made – (if necessary).

3.3.4 Planning The Study

The project team will now draw up a programme of work, with clearly defined timescales and lines of responsibility. A level of flexibility should be built in to allow for the fact that feasibility studies often need to cover a wider range of activities than was initially envisaged.

3.3.5 Problem Definition And Information Gathering

The next stage will produce a formal list of the system requirements, constraints and problems. This will require the gathering of a greate deal of information. In many organizations, the requirements of the system and the way that data flows through the organization will be recorded using specific diagrammatic models.

The list of problems and requirements is likely to cover the following areas:

(a) Data input to the system;

(b) The output (contents level of details, timing, etc) from the system;

(c) The predicted future volumes of transactions and data to be processed;

(d) Technical feasibility

(e) The organizational structure of the user departments and their support staff;

(f) The operational costs of the current system; and

(g) The current hardware and software available, together with a list of the current applications using the hardware and software

At the end of this stage, a set of documents should have been produced, defining the problem/requirements of the system.

3.4 ASSESSING FEASIBILITY

Before it can be considered feasible, a project should be justified on the following grounds:

(a) Technical feasibility

(b) Operational feasibility

(c) Social feasibility

(d) Economic feasibility (costs and benefits).

3.4.1 Technical

The organization must have the technological ability to cope with the requirement of the system. The hardware and software must be capable of dealing with the volume of transactions and required response time without any disruption to business operations.

A technical feasibility study is therefore concerned mainly with specifying the performance requirement of the system, and then assessing whether a proposed new system will be able to meet those performance specifications. For example:

a) Therefore might be a requirement for the system to respond to update a customer's account by the user within a maximum time limit, say 10 seconds. A technical feasibility study would assess whether the hardware files, software and communication links in the proposed system would be sufficient for this performance requirement to be met.

b) Similarly, there might be a requirement to process certain volumes of input transactions and for an ability to store certain qualities of data in a particular form, such as, visual records. A check should be made to ensure that any proposed system is capable of handling the planned volumes in the manner required.

c) There might be a requirement for access to central data files by all the employees in the user organization, from a number of countries across the world. If this is a system requirement, the proposed system must be technically capable of delivering it.

3.4.2 Operational Feasibility

The system must fit in with the way that the organization runs its business and plans to run its business in the future. It must be capable of providing each user with the required information in a timely manner. Operational feasibility considers whether proposed solution is desirable within the existing managerial and organizational framework. It assesses the willingness and ability of management, employees, customers, and suppliers to operate, use , and support a proposed system.

There are three key issues in assessing operational feasibility. These are:

a) Can the proposed system be used in the way intended? Will it work properly? For example, a system might require new data to be input by certain staff in the user organization before the end of the day on Monday on each week. In practice, however, these staff might not get the data for input until Wednesday each week, and so cannot input it before then. If this were the case, the operational specification would not be feasible.

b) User attitudes to the new system. Will users respond to the new system in a positive way, or will there be strong resistance to using it. Will the system be used in unintended and unwelcome ways?

c) What is the impact of the new system on the organization?

3.4.3 Social Feasibility

The system must be compatible with the social organization of the company, and the company must be sufficiently sophisticated to be able to deal with the complexity of the system being suggested. Social

feasibility indicates how well a proposed information system support the objectives of an organization's strategic plan for information systems. It studies the way a proposed system will affect organizational structure, and attitudes as well as decision-making and operations.

This can be split into basic areas:

(a) The suggested system should not threaten industrial and personal relations and motivation;

(b) The system must not conflict with the corporate culture and ways of doing business.

(c) The skill and experience within the organization must be at a high enough level to be able to cope with the complexities of the system.

3.4.4 Economic Feasibility (Cost Benefit Analysis)

Economic feasibility appraises whether the benefits of the proposed solution outweigh the costs thus presenting a clear understanding of the business value of proposed systems. The goal is to determine whether expected cost saving, increased revenue, increased profits and reductions in required investment exceed the costs of developing and operating a proposed system. An organization can incur many

different costs in delivering information to its directors, employee, customers and suppliers. These are often very varied. Some may be capable of being estimated with a high degree of accuracy while others may be uncertain. Many benefits will be completely non-measurable.

Examples of benefits are:

(a) **Savings in labour costs:** These may be predictable allowing for uncertainties in future wage rates and so on.

(b) **Benefits due to faster processing**: examples of these might be reduced debtor periods as a result of speedier debtor processing, or reduced buffer stock due to better stock control.

(c) **Better decision making**: A computerized information system provides more targeted and accurate information quicker and cheaper than manual systems. This leads to better managerial decisions. It is generally not possible to put a figure on the value of better managerial decisions. Even if it were, it would be impossible to assign what percentage of this improvement was the result of better information and what was the result of other factors.

(d) **Better customer service:** it will generally not be possible to estimate the economic benefits of either better customer service or more competitive services.

(e) **Error reduction:** The benefits of this can be estimated if current losses associated with erroneous processing are known.

3.4.5 Financial Justification

There are two aspects to costs: development costs and operating costs. There are revenue and capital sides of the development costs.

Development Costs

Systems design and development: cost from the start of the feasibility study until the system is handed over for maintenance. This heading includes all programming and testing.

Installation costs: preparation costs, delivery charges and other costs arising from any new equipment or computer required.

Capital costs: computer equipment required for the application.

Migration Costs

(a) Staff training

(b) File conversions

(c) Systems testing

(d) Parallel running and other changeover costs

Operating Costs

(a) Hardware/software costs

(b) Staff costs

(c) Supplies – stationery etc

(d) System maintenance

(e) Third party services

(f) Space costs

(g) Other

Project Identification

This stage will enable the feasibility study group to suggest various options for the project eliminate unsuitable options and evaluate the others.

The Feasibility Study Report

Outline of a feasibility study report is as follows:

(a) Introduction

(b) **Terms of reference**: this is a statement of what areas the feasibility working party looked at, the scope, when and at whose request.

(c) Description of the existing system.

(d) **System requirements**: the existing system may be inadequate for meeting user requirements; the feasibility report should therefore state what the requirements of the new systems are. It should also explain how the existing system fails to meet them.

(e) **Outlines of the proposed system:** this should state how the system would operate so as to meet the system requirement. It will specify the input to the system and the output and files. It will also specify the hardware, software and staff requirements for operating the proposed system.

(f) **Implementation plans:** A description of how the new system will be implemented.

(g) The likely benefit from the new system

(h) The expected costs of developing, implementing and operating the system.

(i) A cost-benefit analysis of the proposed system.

(j) Expected benefits of the proposed system

(k) Suggested software, hardware and suppliers and cost implications.

(l) Staff training requirements

(m) Suggested implementation timetables

(n) Information about other organizations that are using the proposed system.

(o) Alternative systems considered, and the reasons for rejecting them.

(p) Conclusions and recommendations

3.5.1 Approval of the Project

The steering committee may approve the project (or recommend its acceptance to the Board) if it is justified. In addition to the recommendation of the feasibility study report, the steering committee will also consider the projects priority amongst other projects under consideration, and its technological, economic, operational and social feasibility.

In order for a project to be carried out, the investment criteria set by the organization must be satisfied. Each of the project proposals still under consideration will be the subject of an analysis comparing the cost of developing the system with its likely benefits. In practice, the evaluation of both costs and benefits can be difficult. The different elements of costs may be hard to definite and the benefits may be speculative and hard to qualify.

For example, a new sales system might reduce debtor's collection periods, but by how much? Similarly, a new stocks system should reduce the frequencies of stock out and obsolete stock, but it will be difficult to qualify the savings or the improved reputation that the company should enjoy.

There are different techniques used to evaluate projects. The costs and benefits are estimate over a period while each technique result in the calculation of a measure. These measures can be used to compare different investments, or they can be compared with a target value to see if the investment meets the organizational requirements.

SELF ASSESSMENT EXERCISE

- Identify the scope of feasibility study you know

4.0 CONCLUSION

This unit being comprehensive as it is has supplied you the needed information as regard system development life cycle. You have learnt about how the feasibility study is being investigated. You have also learnt about the scope of feasibility study, formation of the steering committee, setting up the terms of reference, study group formation and planning. The also introduced you to how the feasibility study are assessed, project identification and approval.

5.0 SUMMARY

System development life cycle (SDLC) or software development life cycle refers to the process of developing a new or amending existing information system, and the methodologies employed to develop these systems.

The stages in system development involve: investigation and feasibility study, formation of the steering committee, setting up the terms of reference and others.

The feasibility study define the time and scope for the implementation of the required solution. The steering committee has the objective of

ensure of that resource allocation decisions are effective. The project team will now draw up a programme of work, with clearly defined timescales and lines of responsibility.

6.0 TUTOR MARKED ASSIGNMENT

- In operational feasibility, the system must fit in with the way that the organization runs its business and plans to run its business in the future. Discuss the three key issue in assessing operational feasibility.

Answer To Self Assessment Exercise

Within the feasibility study, the following are addressed:

a. Defining the time and scope for the implementation of the required solution

b. Establishing optimum solution of meeting business needs and general information resources requirements.

c. Identifying IT products that offer solutions to the problem etc.

7.0 REFERENCE/FURTHER READING

Thursday Bram (2003): What is Grid Computing? Conjecture Corporation.

Scott Burns (2008): A Fresh Look at Cloud Computing in Governance

Rebecca T. Mercum (2005): Challenging in Forensic Computing". Communications of the ACM Vol. 48 No. 12.

MODULE FOUR

UNIT ONE: SYSTEM REQUIREMENTS, ANALYSIS AND DESIGN

UNIT TWO: ESTABLISHING SYSTEM OBJECTIVES, INFORMATION REQUIREMENTS AND SOLUTION ALTERNATIVES

UNIT THREE: SYSTEMS INSTALLATION/IMPLEMENTATION AND MAINTENANCE

UNIT FOUR: CRITICAL FACTORS FOR THE SUCCESSFUL IMPLEMENTATION OF A MANAGEMENT INFORMATION SYSTEM

UNIT ONE

SYSTEM REQUIREMENTS, ANALYSIS AND DESIGN

CONTENTS

1.0 INTRODUCTION

After establishing the need for an information system and the feasibility study is completed, the next stage in the system development life cycle is system analysis. The analysis stages involves examining all the facts that have been recorded in order to make a proper assessment of an existing system or a proposed one. All feasible alternatives must be produced and all procedures to examine critically analyzed. In the main, analysis is designed to examine the documentation of the old system with view to achieve the following. Remove undesirable procedures.

Decide on the best approach (where there are several alternatives) to designing the proposed system.

The design stage is the creative stage in system analysis. It therefore calls for the analysts creative ability. The design of a new system should address the following issues. Coding, input, file and storage output, computer runs, flow etc.

2.0 OBJECTIVE OF THE UNITS

Upon successful completion of this unit, you should be able to:

- Define and explain system analysis and design.
- Examine some of the activities in system analysis
- Discuss the steps involved when planning the interview.
- Examine the problems with interview as a channel of information explaining the restructuring of the questionnaires.
- Explaining also the limitation of questionnaires, designing questionnaire observation measuring, elicitation and user workshop.
- Identity background research and special purpose surveys, recoding and evaluation.

3.1 DEFINITION AND MEANING OF SYSTEM REQUIREMENTS ANALYSIS AND INITIAL DESIGN

After establishing the need for information system and the feasibility study is completed, the next stage in the system development cycle is systems analysis. This is when the analyst carries out a detailed investigation of the existing activities in the application area. Requirements analysis describe the activities involved in analyzing the information needs of those that are going to use the information system, the organizational environment, and any system presently being used, as well as developing the functional requirements of a

system that can meet the needs of these users. The user's requirements should be recorded in a document and should be referred to throughout the rest of the system development process to ensure the developing project aligns with user needs and requirements. IS professionals must involve end users in this process to ensure that the new system will function adequately and meets their needs and expectations.

The key to building any large information system is a thorough understanding of the existing organization and system. In its most basic sense, system analysis is a methodical investigation of the problem that the organization will try to solve with an information system. It involves analyzing, in detail, the information needs of an organization, the characteristics and components of the presently utilized information system in order to define the functional requirements of proposed information systems. The purpose of system analysis is to define the problem, identify its causes, specify the solution, and identify the information requirements that must be met by a system solution.

The activities to be carried out in system analysis are highly technical and would require the services of system analyst. These are experts

who translate business problems and requirements into information requirements and system. The system analyst is responsible for analysis, design, and the preparation of a system specification as well as system testing, review and maintenance.

It is important for system analysts to demonstrate the following competencies:

(a) Understanding of the business applications

(b) Ability to communicate with users and

(c) Understanding of technical specifications and programming details.

3.2 ACTIVITIES IN SYSTEMS ANALYSIS

The following activities are involved in system analysis

(a) Data gathering and evaluation

(b) Establishing information requirements and solution alternative and

(c) Selecting the package

3.2.1 Data Gathering and Evaluation

There are basically three activities involved in data gathering and evaluation – fact-finding and data collection, recording and evaluation. In fact-finding, the analyst attempt to learn as much as possible and gathers data about the existing system; recording brings the knowledge about the system together with the data gathered while evaluation appraises the document data.

3.2.2 Fact-finding and data collection

A major part of system investigation is fact-finding and data collection. The system team must find out what the existing information system provides, and how the information is used. Methods of fact finding are discussed below:

3.2.3 Interviews

Interviews involves face-to-face discussion between the analyst and the users, specialist and other individuals with knowledge of the system. The analyst asks questions and obtains answers, comments and suggestions. This is the most important way in which an analyst will obtain information. Setting up interviews with key personnel at all

levels in the org ensures a rich and complete view of what is happening. Interviewing is more of an art than a mechanical technique and improves with experience. There are, however, several guidelines that are recognized as essential to successful interviewing

3.3 PLANNING THE INTERVIEW

Interviews should always be planned, even when conducted in an informal manner. The interviewer needs to plan:

(a) Whom to interview: obviously he or she will be unable to interview everyone unless the project scope is very small. Each user will have different information to offer, and different levels of requirements, depending upon their level in the organization.

(b) When to interview: there is the need to avoid times which will be particularly disruptive to the day to day business of the company. The interview should being neither too early nor too late. Timing will depend in part on the number of interviewers to be conducted.

(c) What to ask: the questions asked will depend on the requirements of the proposed system, and user's feedback

reflecting their own needs and concerns. Background information on the current workings of the system, and any problems arising, is also important.

(d) Where to interview: if the interviewee will need to demonstrate his/her tasks or refer to documentation, then the interview is best conducted at the location on the interviewee. This also serves to put the interviewee more at ease, as well as allowing the analyst opportunity to informally observe aspects of the workplace.

(e) How to being the interview: will a formal or informal approach be best suited to the interviewee? What is the best way to obtain the interviewee's confidence?

(f) How to analyze the notes, recording etc made during the interview.

3.31 Before the interview

Whether to interview formally or informally by conducting a structured or unstructured interview will depend upon the type of person being interviewed and the atmosphere the interviewer wishes to create:

(a) The analyst must have a clear purpose for each interview undertaken, that is, the analyst should establish in advance the missing information that the interview is meant to supply.

(b) Interviewers must have background information on those interviewed and many find this valuable later on during implementation. It give an opportunity to discuss in-depth opinion and he may learn of suggestions that are worth further looking into.

(c) The analysts should prepare thoroughly for the interview by becoming familiar with technical terms that are likely to be used by the interviewees and with their positions and general responsibilities.

(d) The analyst should also outline a list of questions to be asked during the interview.

3.32 During the Interview

(a) Explain at the beginning the purpose of the interview. This gives the interviewee a framework of reference for answering questions.

(b) Attempt to put the interviewee at ease.

(c) Go through the questions that were prepared. General questions should be asked first followed by more specific questions on each topic area. The analysts should always listen carefully to replies and be able to follow up answers with questions that were not in the original list. The analysts must always bear in mind the purpose of the interview and discourage time-washing diversions.

(d) Never condemn the interviewee. The analysts is merely seeking information.

(e) Not to enter into a discussion of the various merits or weaknesses of other personnel in the organization.

(f) Summarize points made by the interviewee at suitable stages in the interview.

(g) Explain the purpose of note taking or a tape recorder, if used.

(h) Keep the interviews short; generally 20 minutes or half an hour may be sufficient.

(i) Summarize the main points of the interview at the end.

(j) Book a follow- up interview, if required, with the interviewee at the end of the interview.

3.33 Problems with interview as a channel of information

The interview, though the most valuable tool for information gathering for the analyst, is limited in that:

(a) The interviewee may refuse to cooperate with the interviewer through fear or job loss, redundancy, or the inability to cope with the new technology as a result of computerization. This may take the form of a direct refusal to take part, being vague in replies, by omission, or continuing to let the analyst believe what the interviewee knows to be false.

(b) Interviewing is an acquired skill and depends upon the cooperation of those being interviewed. It can be costly in time and effort and the result are unpredictable.

(c) It is extremely time-consuming for the analyst.

As a fact-finding technique, interviewing is appropriate in almost all situations. It may be particularly useful where the proposed system will involve a number of related areas in the existing system. This is because it is usually only by talking to all parties involved that the analyst will gain a total view and proper understanding of the interaction of the various parts of the system. Face-to-face interview is an excellent way to obtain detailed, in depth information. It is one

of the major investigative methods and requires good communication skills from the analyst.

3.4 QUESTIONNAIRES

Questionnaires are written lists of questions given to employees and management. These can be used by a system analyst in an interview, or given to respondents, who will be asked to write answers in their own time and return the completed questionnaire.

In many ways, the ideal solution to the problem of fact-finding will involve a certain amount of direct contact between the analyst and those members of staff concerned with the day-today running of the system. However, it may sometimes be physically impossible, or at least highly impractical, for the analyst to personally talk with all staff members. This may be because the number of staff involved and/or the decentralized nature of the business organization. It is in such situations that the use of questionnaires may have to be considered.

Questionnaires can sample a wide range of opinions and collect useful statistics in a short space of time. Particularly if those questioned cover a large geographical area. There are many problems with questionnaire. The response rate may be poor, analysis of a lengthy questionnaire

can be costly and design of a good questionnaire is not easy, particularly if consistency of answers is needed to be checked by cross-referencing answers.

Where questionnaires are to be distributed for completion by staff members, it is essential that the questions themselves have been designed in such a way that ambiguities are avoided. There is also a danger with questionnaires that staff may give the reply that they feel is expected of them, rather than what they see as the answer in 'real life'. For these reasons, questionnaires should only be used where the system details which the analyst is enquiring about are comparatively simple.

3.4.1 Limitation of questionnaires

Certain limited situations may make a questionnaire suitable. These usually occur when the number of people involved makes interviewing prohibitively expensive, the questions are generally simple, a low response rate is satisfactory, and the questionnaire is used to confirm is used to confirm evidence collected elsewhere. Questionnaires are of only limited use in obtaining information for the purpose of investigating an existing system (as opposed to market research where they are essential). This is because:

(a) It is difficult to avoid misunderstanding on the part of respondents as they cannot gain clarification of a question on the questionnaire if it is judged to be vague or confusing.

(b) Questionnaire that are simple provide little information; questionnaires that are more ambiguous are likely to be misunderstood.

(c) Responses rates to questionnaires are often low.

(d) To design a good questionnaire, the analyst often needs more information about the system under investigation than the questionnaire could hope to provide in the first place.

3.4.2 Designing questionnaires

Questionnaires can be used to collect large amounts of information from large number of people. Questionnaires must be properly designed in order to extract meaningful information. In designing questionnaires, it is important that the following factors should be considered:

(a) Align the tone and style of the questionnaires to the objective of the questionnaires

(b) Keep questions simple, short, unambiguous, unbiased and straight to the point.

(c) Use multiple –choice questions rather than asks for comments. This makes the questionnaire both easier to answer and easier to analyse.

(d) Have a clear idea of the information that is required from the questionnaire.

(e) Make sure that the questions align with the level of intellect and particular interest of the respondents.

(f) Avoid branching: for example, ' if your answer to question 8 was 'yes' then go to question 23 otherwise go to question 19'.

(g) Make clear the deadline date by which the questionnaire is to be returned and enclose an addressed and prepaid envelope.

(h) Decide in advance how responses will be analysed and the timescale for return.

3.4.3 Observation

Observation involves the analyst watching the system in operation and inspection of current reports and files as an observer. Observational

studies include formal observation of a task, shadowing a user through their working day and participating within the user environment.

Studying by observation requires some level of knowledge about the system and should provide experience of the details of the system that is needed if changes are to be introduced. It can be a cheap means of gaining knowledge of a system and have the advantage of showing what actually happens, not what one expects or believe to be happening.

On the other hand, direct observation is time-consuming and may provoke a reaction in those observed which makes it difficult to allow normal working practice to go ahead as normal. It is for this reason that it would perhaps be necessary to make a number of separate observations at random intervals, rather than forming an opinion based upon a single visit.

Observation is useful 'follow-up' procedure, used to gain conformation that a system as outlined 'in theory', perhaps in an interview, does actually work in practice. It might be used whenever the flows of documents through a system need to be assessed for efficiency. It is however an important source for the analyst on informal information flows between individuals. These are often essential for the efficient

execution of activities. They may be obvious from interviews and would not appear in documentation.

The analyst will watch the current system in operation. When investigating by means of observation, it must be realized that the result will be distorted by the observation activity itself. Human nature dictates that different behaviour will occur when an individual is away that he is being observed thus devaluing the information obtained. Observation, unlike interviewing, does not reveal the beliefs and attitude of the people involved.

3.4.4 Measuring

Sometimes it is important to have statistical information about the operations of the existing system. The total number of sales ledger accounts and the activity of each will be of interest to the analyst who is looking at the possible computerization of an accounting system. The statistical spread as well as the gross figures may be relevant. For instance, with a sales order processing system, not only may the average number of sales orders processed in a day be of use to the analyst, but the pattern of these orders throughout the day and throughout the week may be of significance. Are there peaks and troughs or is it a constant flow?

3.4.5 Elicitation

Elicitation is concerned with extracting from a group of users a description of the requirements for a system from the users' point of view. Building this picture of requirements has three stages.

Firstly, identification of the information sources that will be used to provide details about the system, in terms of people and documents. Existing documentation such as organization charts and procedure manuals can be used to try and check the completeness of this list of sources.

Secondly, establishing the relationships between the information sources that have been identified. It is important to establish both direct relationships (where information passes from our user to another) and hierarchical relationship (where one user carries out part of the actions of another user). The information flows in particular need to be correctly documented. Lastly, elicitation can take place by analyzing documents and performing user interviews.

User Workshop

Information concerning user requirements can also be obtained in a user workshop. The main purpose of this activity is to discuss with users as a group their requirements for a system. Making the collection of data part of a discussion will help to improve the accuracy of the data collected because the users will start to see how, for example, outputs from one department of the organization will start to affect other departments. This type of workshop is known as a joint requirements planning workshop, or JRP.

3.4.6 Background Research

Information about a system will also be available from other sources such as questionnaires and studying documents that are used within a system. Information is sometimes available in the form of written instructions or procedures manuals. The system analysts should study these to become familiar with the system and avoid asking elementary questions at interviews. Information obtained from such sources should be treated with caution, as it is often out of date or misleading.

Special purpose surveys

These are designed by the analyst to gain extra data about the current operations of the system. For example, to establish how long a clerk

spends in a day in a particular tasks. A special purpose survey will ask that clerk to record exactly when the tasks begins and when it finishes, for a period of a week or fortnight or whatever is suitable. From this, the analyst can identify peaks and troughs in this activity, and measure its impact on the rest of the system. This is useful for calculating how much time can be saved if the task is to be performed by the new computer system. Special purpose surveys are a way of sampling the activities carried out by the users, in order to find out how much time is spent, on average, on each task.

3.4.7 Recording

Fact- finding leaves the system analysts with a large amount of information, often in disordered form. The information now has to be properly recorded. This recording will take the form of procedure narrative, flow charts and decision tables.

The analyst now has to prepare documentation of the existing system. This should include:

(a) Source of information (people interviewed, documents studied etc);

(b) A narrative description/summary of the system;

(c) Comments on the system, with particular attention to any weaknesses e.g. errors, delays, excessive costs, bottlenecks etc;

(d) Recommendations for improvements;

(e) Flowchart (s) and data flows of the system processes;

(f) Specimen document

(g) Organization charts

(h) Staff numbers, work volumes, costs etc; and

(i) Graphs, bar charts and diagrams, where appropriate.

This report serves as a record of the existing procedure. It may be checked by a senior system analyst to ensure that everything has been covered. It is used as the basis of subsequent systems design.

Evaluation

In order to carry out effective requirement analysis, a critical evaluation of the findings at the data gathering process must be carried out. The existing system can now be reviewed critically to assess the need for data, processing procedures and costs. In this process, the problems, inefficient s and bottlenecks in the existing system are identified and steps to correct them are formulated.

The final stage of systems investigation is to analyse the findings, in order to learnt the inadequacies of the existing system. Analysis provides the link between systems investigation and systems development, is it only by learning why existing procedures are inadequate and comparing them with management's declared information requirements that an improved system can be developed.

Concerning the structure of the system, the evaluation should provide answers to questions such as:

(a) What are the subsystems within the overall system;

(b) What is the flow of inputs (men, money, machines, materials) and outputs; and

(c) What information is provided for decision-making, and what decisions are made (and by whom).

Concerning the environment of the system, evaluation should address the following:

a) What are the influence of the environment outside the business;

b) If the problem is concentrated on just one area of the business, some analysis will be required of other parts of the wider business system.

c) The objectives of this wider environment must be analyzed, so that the potential conflicts between them and the objectives of the system under investigation can be identified

SELF ASSESSMENT EXERCISE

- Briefly discuss the factors that are to be considered when designing questionnaires

4.0 CONCLUSION

In this unit, you have learnt about system analysis definition, the stages involved, the activities in system analysis, planning the interview (before the interview). This unit has also taught you the associated problems with interview as a channel of information, designing the questionnaire and its limitations. The unit also shows up the factors to be taken cognizance of when designing the questionnaire.

5.0 SUMMARY

The activities to be carried out in system analysis are highly technical and would require the services of the system analysts. These are experts who translate business problems and requirements into information requirements and system.

It is important for system analysts to demonstrate the understanding of the business applications; ability to communicate with users, and understanding of technical specifications and programming details. Date gathering and evaluation and selecting the package are good examples of activities in systems analysis.

When planning the interview, questions such as whom to interview, when to interview, what to ask, where to interview and how to begin the interview arise.

6.0 TUTOR MARKED ASSIGNMENT

* Briefly discus the problems associated with interview as a channel of information.

Answer To Self Assessment Exercise

When designing the questionnaire,

a. Align the tone and style of the questionnaire to the objective of the questionnaires.

b. Keep questions simple short, unambiguous, unbiased and straight to the point.

c. Use multiple choice questions, rather than asks for comments

d. Decide in advance how responses will be analyzed and the timescale for return.

7.0 REFERENCE/FURTHER READING

I. K. Oyeyinka (2006): Introduction to Management Information Systems; 2nd Edition, Printed by Famworks Printers.

Taiwo Olayanju (2005): Basic Computer Studies for Schools and Colleges, Daban Printers.

Ojajuni Jethro (2009): Computer and Business Information System, Published By Boomart ScmS Ltd.

UNIT TWO

ESTABLISHING SYSTEM OBJECTIVES, INFORMATION REQUIREMENTS AND SOLUTION ALTERNATIVES

CONTENT

1.0 INTRODUCTION

As a result of these studies, it should be possible to formulate a list of objectives of the system under investigation, these objectives should, where possible, be measurable in quantitative terms so that performance indicators can be set up to check whether actual results achieve the objectives. It is especially important that the objectives of the system should conform the overall objectives of the business, and where appropriate make an optimal compromise with the objectives for the external environment of the whole business. Having establish

the objectives of the system, it would then be necessary to decide what information must be provided to help managers achieve them.

The primary purpose of system analysis is to define the specific information requirements that must be met by the system solution selected. This involves defining the objectives of the proposed system and developing detailed descriptions of the functions that the new system must perform. Requirement specification must be sound and through if the final system must perform up to expectations.

2.0 OBJECTIVE OF THE UNIT

At the end of this unit, you are expected to do the following at ease:

- Define and explain system requirement
- Ascertain the key examples of functional requirements
- Selecting software packages and functions included.
- Analyze detail system design specification/documentation.
- Evaluate the objectives of system design.
- Explain the logical and physical design of system
- Assess the essential content of a system specification

- Identify and dilate copious program specifications

3.1 REQUIREMENTS/DEFINITION AND MEANING

As a result of these studies, it should be possible to formulate a list of objectives of the system under investigation. These objectives should, where possible, be measurable in quantitative terms so that performance indicators can be set up to check whether actual results achieve the objectives. It is especially important that the objectives of the system should conform to the overall objectives of the business, and where appropriate make an optimal compromise with the objectives of the external environment of the whole business. Having established the objectives of the system, it would then be necessary to decide what information must be provided to help managers achieve them.

The primary purpose of system analysis is to define the specific information requirements that must be met by the system solution selected. This involves defining the objectives of the proposed system and developing detailed descriptions of the function that they new system must perform. Requirement specification must be sound and thorough if the final system must perform up to expectation.

Requirement definition

Requirements definition is concerned with the identifying and specifying the business requirements of the system chosen for development during the feasibility study. Requirements include description of what a system should do, how users will interact with a system, conditions under which the system will operate, and the information criteria the system should meet. The requirements definition phase also deals with issue associated with effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability which are sometimes called non-functional requirement.

3.1.1 Examples of Functional requirements

(a) User interface requirements: Automatic entry of product data and easy –to-use data entry screens for customers.

(b) Processing requirements: Fast, automatic calculation of sales totals and delivery costs.

(c) Storage requirements: Fast retrieval and update of data from product, pricing, and customer databases.

(d) Control requirements: Signals for data entry errors and quick confirmation for customers.

In order to accomplish the above in the requirements definition phase, the following activities must be carried out:

(a) Identify and consult stakeholders to determine their expectations.

(b) Analyze requirements to detect and correct conflicts and determine priorities.

(c) Identify system boundary and how the system should interact with its eternal environment.

(d) Convert users requirements into system requirements (e.g., an interactive user interface prototype that demonstrates screen look and feel).

(e) Verify that requirements are complete, consistent unambiguous, verifiable, modifiable, testable and traceable. In view of the high cost of rectifying requirements problems in systems development phases, effective requirements reviews have a large payoff.

(f) Resolve conflicts between stakeholders.

(g) Resolve conflict between the requirements set and the resources that are available.

(h) Verify and validate information on requirements

3.1.2 Selecting Software Packages

Application software packages must be thoroughly evaluated before they can be used as the foundation of a new information system. The most important evaluation criteria are the functions provide by the package, flexibility, user friendliness hardware, documentation, vendor quality and cost.

The package evaluation process is often based on a request for proposal (RFP), which is a detailed list of questions submitted to vendors of packaged software.

Request for proposal (RFP)

RFP are detailed lists of questions submitted to vendors of packaged software or other computer services to determine if the vendor's product can meet the specific requirements of the organization.

Functions included

The functions included vary by application. But for the specific application, the following considerations are important:

(a) How many of the functional requirements will the package meet?

(b) Which functions can be supported only by modifying the package code?

(c) How extensive are the modifications required?

(d) Which functions cannot be support at all by the package?

(e) How well will the package support future and current needs?

Flexibility

(a) How easy is the package to modify?

(b) What customization features are included?

(c) Is the vendor willing to modify the software for the client?

Users friendliness

(a) How easy is the package to use from a non-technical standpoint?

(b) How much training is required to understand the package?

(c) How much user control does the package allow?

Hardware And Software Resources

(a) On what kind of computer can the package run?

(b) What operating system is required?

(c) How much CPU and storage resources does the package utilize?

(d) How much computer time is needed to run the package?

Database/File Characteristics

(a) What kind of database/file structure does the package use?

(b) Do the standard fields in the package file correspond to the data elements specified the application requirements?

(c) Does the database or file design support the client's processing and retrieval requirements?

(d) Are there provisions to add customized user fields for data elements that are not standard with the package?

3.3 DETAILED DESIGN SPECIFICATION/DOCUMENTATION

While system analysis describes what a system should do to meet information requirements, system design shows how the system will fulfill this objectives are met. The design of an information system is the blue print or model for that system and consists of all specifications that give the system its form and structure. In practical terms, system design details how a system will meet the information requirements as determine by the system analysis.

3.1.3 The objectives of system design are as follows:

(a) System design is responsible for considering different technology configurations for carrying out and developing the system as described in system analysis by the analyst. This will include evaluating different hardware and software components, security and networking capabilities.

(b) System design is responsible for the management and control of the technical formation of the system. This include detailed programming specifications, data coding, acquisition of software as well as hardware testing and training.

(c) System design is responsible for detailing the system specifications that will produce the functions defined in system analysis.

System design includes activities such as:

i. Creating logical design specifications

ii. Creating physical design specifications

iii. Managing the technical formation of system

iv. Translating design specifications into program code

v. Configuring the package to user requirements

vi. Training technical staff on the package and

vii. Redesigning organizational procedures.

3.3.2 **Logical** and physical design: It is possible to describe a system in a number of ways. A system can be analyzed in terms of its components (that is, a collection of hardware and software items) otherwise known as physical design. Alternatively, a system can be examined in terms of what is does (that is, the detail of the processing operations it performs). Finally, a system can be viewed abstractly, in terms of its logical design. Theoretically, it is not impossible for one logical design to be implemented in more than one physical way (such as, use of different hardwares or different programming languages.

Logical design: the logical design of a system is the design of the system in concept, what the system is meant to achieve, rather than detailed implementation. Logical design lays out the components of the system and their relationship to each other as they would appear to users. It shows what the system solution will do as opposed to how it is actually implemented physically. It describes inputs and output, processing functions to be performed and business procedures as well as data models and control.

Once the analysis is complete, the analyst has a good idea of what is logically required of the new system. There will be a number of ways that this logical models can be incorporated into a physical design. For instance.

(a) Is the data storage to be implemented as a series of files or is there to be a database? Should this be centralized or distributed?

(b) How many of the processes are to be incorporated into a computer system and how many are to remain manual?

(c) Of those to be computerized, which are to be run under batch processes and which interactively online?

(d) Is the computerized system to be centralized or distributed?

There will not be one correct answer to these questions. Rather, there will be a range of alternative designs with different cost and efficiency implications. Some will yield more computerized facilities than others. The analyst will suggest two or three design alternatives to management together with their implications. Management will then decide amongst them. Often these alternatives will reflect a low – a medium – and a high –cost solution to the problem. The first will provide a system that is very basic. The second alternative will incorporate more facilities while the third may go beyond this to

illustrate the full potential of extensive computerization. This stage ends with a choice between the alternatives presented to management.

Physical design: The physical design of the system not only specifies hardware, but also the exact design as to how a particular procedure will be implemented in software. Physical design is the process of translating the abstract logical model into the specific technical design fro the new system. It produces the actual specifications for hardware, software and physical databases as well as input/output media, manual procedures and specific controls. Physical design provide the specifications that transform the abstract logical design plan into a functioning system of people and machines. Detailed physical specifications need to be made so that the system can be purchase/built and installed. There are a number of distinct areas that must be considered:

The analyst will specify details of the systems being developed. The design is broadly based on that suggested during the feasibility study but will go into considerable detail:

(a) Data input, processes and outputs;

(b) File structures

(c) Program specifications for each program in the system

(d) A test schedule for each program

(e) A test schedule for overall system

(f) The method of implementation

(g) A detailed time schedule for hardware/software acquisition or creation

(h) Operating instructions

(i) Training schedule for users; and

(j) System performance measurement

At this stage, a system specifications will be produced, specifying what the chosen option of new system will look like. This requirement specification can be distributed to potential writers of the software or suppliers of software packages. This document will also form part of the invitation to tender (ITT) which is sent out to suppliers. Responses to the invitation to tender will have to be evaluated and a supplier chosen.

3.4 SYSTEM SPECIATION

Whether the system is manual, partly computerized or wholly computerized, the design team should prepare a system specification which describes the terms of reference, the proposed new system (inputs, output, file procedures, technical equipment) and the cost-benefit analysis, together with a timetable for design and implementation. This contains a description of the alternative systems considered and how far each of these would satisfy the objectives. Alternatives which fail to satisfy those objective should be explained, and then discarded from further consideration in the report.

The system specification is a complete documentation of the whole system and must always be properly updated as parts of the systems are changed or added to. Many of the problems in computer installations arise because of inadequate systems well as program documentation and controls. The detailed system specification will provide the basis for programming, in the case of a computerized system. The system shows how the organizational requirements specified by the user will be delivered by a computer –based solution. Part of this design will be the detailed specifications of processes.

System specifications formalize the design of an applications' user interface methods and products, database structures, and processing

and control procedures. Therefore, system designers will frequently develop hardware, software, network, data and personnel specifications for a proposed system.

3.4.1 Advantages of systems specifications are as follows:

(a) System specification progresses system design to implementation where top management makes significant commitments to the project.

(b) System specifications provides the source documentation from which programs are written and hardware tenders are prepared.

(c) The system specification provides the source documentation from which programs are written and hardware tenders are prepared.

(d) The system specifications document acts as a historical record of the system specification document acts as a historical record of the system for future users and developers. As an entire documentations of the whole system, it must always be kept up to date as parts of the system are changed or added to it.

(d) System specification provides a point of reference used in the assessment of the system once the system is being used.

3.4.2 Essential contents of a system specification

This is also called the "structure of a system specification". In an outline, the essential contents are:

(e) Introduction

i. System summary

ii. Objectives and benefit and

iii. Hardware and software requirements

(f) System definition (system description)

iv. Narrative description in non-technical language.

v. They system flowchart

(g) Input Specification

i. Summary of input document description and layout

ii. Input media description and layout

iii. Input controls and

iv. Data capture procedure

(h) File Specification

i. Summary of file description

ii. Record layouts and

iii. File processing and file controls.

(i) Output Specification

i. Summary of output descriptions and layout

ii. Report mock-ups

iii. Report handling and distribution procedures and

iv. Output controls

(j) Program Description (Program Specification)

i. The main tasks to be perform by the programs

ii. Computation logic

iii. Special formula ; and

iv. Test data

(g) Implementation procedure

(i) Preparation of job procedures for computer and user requirements

(ii) File creation and

(iii) Changeover procedures

(h) Time Table

(i) User department instructions; and

(ii) Clerical procedures

(i) Appendices

(i) Definition of term; and

(ii) Record reference codes

3.5 SYSTEM DOCUMENTATION

Basically, system documentation refers to descriptions of how an information system works from both a technical and an end –user's standpoint. It is a collection of documents that describe the system, its components, the data, and records of changes made to the system. They are aids provided for understanding the structure and intended uses of an information system or its components, such as flowcharts, textual material, and user manuals. Comprehensive documentation will include the requirements, capabilities and limitations such as design, operation and maintenance guides for the system.

The word 'documentation' refers to a very wide range of reference materials used in the running and maintaining computer systems. It takes various forms ranging from the very technical to the completely non-technical books, manuals, descriptions and diagrams relating to the use and operations of a computer system. Examples include user manuals, hardware and operating software manuals, system specifications and program documentation. The nature, size and scope of a system determine the optimum amount and scope of documentation.

The following points summarize the need for good system documentation:

(k) To enable d analyst, programmers, users and computer operators to communicate;

(l) To facilitate revision or modification of system

(m) For use in the training of system operation staff

(n) To assist in the detection and correction of errors in the systems

(o) To ensure consistent application of system throughout the organization;

(p) To assist the auditor in the computer audit process.

3.5.1 Types of documentation

The first category of documentation that must be kept is that which was used in the initial system development process. These are the feasibility studies, system specification and program specification was well as test data and security precautions.

Details of all changes to the system must be recorded and documented to the same standard as the original system. Copies of all documentation must be updated when changes are made. Costly errors often occur when an organization operates a system using an outdated manual. It is desirable that organizations require that changes are justified and authorized formally.

The second category of documentation is that aimed at helping the users. It includes users manuals, help screens, handy reference cards, and various other references designed to make life easier for the users.

3.5.2 Technical manual

The technical manual is designed to be used by future project teams who may need to fix, modify or upgrade the system. For this reason, its language will be far more technical than that of the user manual and its contents will differ.

A technical manual might contain the following:

a) System objectives

b) Systems overview

c) Performance specification

d) Technical specification

e) Appendices

f) Data dictionary

g) Dataflow diagrams, entity models and life histories

h) Program specifications

i) Likely upgrades and fixed required in the future; and

j) Contact details for the original designers and developers

3.6 PROGRAM SPECIFICATIONS

A program specification, or program documentation is the complete description of a program. It usually includes notes, flowcharts, program listing, test data and expected results. The systems analyst draws up program specifications. A copy of the program specification is given to the programmer responsible for writing it, and the programmer then uses the specification as the basis of writing and testing the required program. When the program has been written and tested, one copy of the final specification will form part of the overall system specification, and a second copy will be retained by the programmer to form part of the programmers' own documentation for the program. There should be a program specification for every individual program in the system.

3.6.1 Computer operation manual

This manual provides full documentation of the operational procedures necessary for the 'hands-on' running of the system. Amongst the matters to be conversed by this documentation would be the following:

(q) Systems set-up procedure: Full details should be given for each application of the necessary file handling and stationery requirements etc.

(r) Security procedures: particular stress should be placed on the need to check that proper authorization has been given for processing operations and the need to restrict the use of the systems to authorized operators.

(s) Reconstruction control procedures: Precise instructions should be given in relation to matters such as hard disk crash and also the recovery procedures to be adopted in the events of a system failure.

(t) System messages: A listing of all message like to appear on the operator's screen should be given together with an indication of the responses which they should evoke. The screen, with associated keyboard or mouse, is the means by which the operator will communicate with the computer, and respond to such computer messages as error conditions.

(u) Operating system manuals: These are manuals that explain the use of an operating system.

3.6.2 User manual

During the development of a system, it will be necessary to produce documentation to support the system in use, and to aid further development or modification. The user manual is designed to support the training of users, and to provide them with a reference guide in case they experience problems during the operation of the system.

The user manual will be written in non-technical language, and will normally include the following sections:

i. System objectives;
ii. System overview;
iii. Input stage activities
iv. Process and storage activities
v. Output on the screen
vi. Report
vii. Appendices, with a completion guide
viii. Sample reports
ix. Error messages, and what to do about them
x. Fault reporting procedures; and

xi. Support details and help desk contact numbers

User manuals or user documentation is that part of the full documentation relating to a program which gives the user information necessary for the successful running of the program but do not include the program specification. The user manual is written to explain the system to the users whose need to be aware of their own responsibilities. Matters to be dealt with should include the following:

(a) Acceptance testing: The preparation of test data and subsequently checking the test results.

(b) Input: Responsibilities and procedures for preparation of input.

(c) Error handling procedures: full explanation of nature and form of error reports and instructions as to the necessary action to be taken.

(d) Master file amendment procedures: Full explanation of necessary authorization and documentation required for file amendment.

(e) Output: What the output is, the form it takes and what should be done with it.

3.6.3 System changes manual

Amendments to the original system specification will almost inevitably occur, in addition to the computerization of additional company activities. The objective of the system changes manual is to ensure that such changes are just as strictly controlled, as was the case with the original systems development and introduction. Four matters to be covered in this respect would be as follows:

(v) Recording of the request and reasons for a change

(w) Procedures for the authorization of changes.

(x) Procedures for the documentation of changes.

(y) Procedures for the testing of changes.

SELF ASSESSMENT EXERCISE

- List some of the examples of functional requirements you know and write short note on each.

4.0 CONCLUSION

This unit is considered extremely paramount to information and communication technology. You have learnt about the definition and meaning of system requirements, the examples of functional requirements, selecting software packages and details design specification/documentation. You have also learnt about system specification, the advantages of systems specifications and types of documentation and program specifications.

5.0 SUMMARY

System requirements definition is concerned with identifying and specifying the business requirements of the system chosen for development during the feasibility study. Requirement include descriptions of what a system should do, how users will interact with a system conditions under which the system will operate, and the information criteria the system should meet.

Functional requirements and control requirements. System design include activities such as creating logical design specification creating and managing the technical formation of system among others.

One of the advantages of system specification is that progressed system design implementation enables top management makes significant

commitment to the project. The essential contents of a system specification - introduction, system definition/description, input specification, file specification etc.

6.0 TUTOR MARKED ASSIGNMENT

- What is system documentation? What do you think could be adduced reasons for system documentation?

Answer To Self Assessment Exercise

vi. Functional, requirements: automatic entry of product data and easy use data entry screens for customer.

vii. Processor requirements, storage requirements and control requirements. Processing requirements involve; fast automatic calculation of sale totals and delivery costs.

7.0 REFERENCES/ FURTHER READING

I. K. Oyeyinka (2006): Introduction to Management Information Systems; 2nd Edition, Printed by Famworks Printers.

Taiwo Olayanju (2005): Basic Computer Studies for Schools and Colleges, Daban Printers.

Ojajuni Jethro (2009): Computer and Business Information System, Published By Boomart SCMS Ltd.

UNIT THREE

SYSTEMS INSTALLATION/IMPLEMENTATION AND MAINTENANCE

CONTENTS

1.0 INTRODUCTION

With the agreement of systems specification by senior management, activities required to put the planned system into action can begin. Implementation activities are needed to transform a newly developed information system into an operational system for end users. The activities involved in system implementation stage include; acquisition and development of hardware, software and services, end user training, testing and installations; system documentation; file conversion, and system changeover from an organization to get as much out of technology as it can, computer literacy must spread throughout all levels of the organization.

The issue of training becomes compelling in order to make personal at all levels competent willing to use IT. Training is a key part of the implementation of a new system. It takes the form; traditional classroom lectures, computer base training involving on-screen practice on the computer etc.

Testing examines the system in order to ensure that all that needs to be built into it had been done to specification by assessing it for how it performs in a 'live' environment. The files must be created before the system is operational. File creation or file conversion is always a major

practical problem when a new computer- based system is being implemented. Planning a file conversion can also involve setting a timetable for conversion etc. The major approaches to changeover involve direct changeover, parallel running, phased changeover.

2.0 OBJECTIVE OF THE UNIT

Having carefully studied this unit, you should be able to:

- Discuss succinctly the nature of systems installation/implementation and maintenance.
- Explain the acquisition and development of hardware and software
- Identify the advantages and disadvantages of off-the-shelf packages.
- Show in detail the merits and de-merit of bespoke systems.
- Examine system installation training and those issues surrounding it.
- Discuss file creation and conversion and the various approaches to change over.
- Elucidate on the common strategy formulation and deciding on the method of change over.

3.1 NATURE OF SYSTEM INSTALLATION/IMPLEMENTATION MAINTENANCE

With the agreement of system specification by senior management, activities required to put the planned system into action can being. Implementation activities are needed to transform a newly developed information system into an operational system for end users. The implementation stage of a computer system can be considered to be a project in it own right. It is the stage when the theoretical design becomes a working, practical system. It is normal to encounter system; the more complex the system, the greater the likely number of problems. To some extent, the problems will be unavoidable. Many, however, can be avoided by proper planning and control.

Activities involved in this stage include:

(a) Acquisition and development of hardware, software and services

(b) End users training

(c) Testing and installations

(d) System documentation

(e) File conversion and

(f) System changeover

The tasks are separate but related and they must all be accomplished even though they may be carried out simultaneously.

3.2 HARDWARE/SOFTWARE ACQUISITION AND DEVELOPMENT

Software packages: A software package is a comprehensive software solution usually developed by software companies for sale to an unrestricted business community. Software packages are normally developed for common business applications, such as accounts and payroll, and these are offered for sale to prospective purchasers. The software is not developed against specific requirements (as in a bespoke solution), but is developed to provide a range of facilities usually required in a business application. It is the responsibility of the buyer to ensure that the functionality of the software fits the specific requirements of their own organization.

A bespoke solution is where a software system has been specifically developed to fulfill a defined business requirement for a specific organization. In this approach, the business develops a functional specification defining the business requirements of the system.

3.2.1 Buying Software

There is a long checklist of point to consider when choosing a suitable package. Some of them are outlined below:

(a) Whether the package fits the user's requirements such as report production, anticipated volume of data, data validation routines and any other specification.

(b) Whether the package comes with useful 'add-on' facilities, such as, report generation facilities

(c) Whether the processing time and response time is fast enough

(d) Availability of full and clear documentation of the package

(e) Ability of the supplier/dealer to demonstrate the package

(f) Ease of use and user friendliness of the package – availability of menus, on-screen prompts and help facilities;

(g) Adequacy of controls included in the package (such as passwords, data validation checks, accounting controls and reconciliation as well as audit trail facilities)

(h) Provisions for updating or amending or modifying the package

(i) Survey of other users of the package and how long it has been in the market.

(j) Compatibility with existing hardware

(k) Support and maintenance service to be provided by the software supplier; and

(l) Cost effectiveness of the package

3.2.2 Advantages off-the- Shelf Packages

The advantages of using an' off-the-shelf' package as opposed to designing a system from scratch are as follows:

(a) It would have been written by software specialists and so would be of high quality.

(b) A successful package will be continually updated by the software developer, and so the version that a customer buys should be current.

(c) Other users will have used the package already and a well-established package should be error-free and well suited to the general needs of users.

(d) Good packages are well documented, with easy to follow user manuals. Good documentation is a key feature of successful software development.

(e) The computer user does not need to employ his own specialist staff to develop, write and test 'in-house' programs, which could take time to produce and would be costly.

(f) Some packages can be tailored to the user's specific needs.

(g) They are generally cheaper to buy than bespoke packages if are to be developed.

(h) Any system bugs should have been discovered by the vendors before sale.

(i) Good packages are likely to come with good training programs, excellent documentation and on-screen help facilities.

(j) New updated version of the software are likely to be available on a regular basis.

(k) The experience of a great number of users will similar needs to those in the organization has been incorporated into design of the package.

(l) Different packages will be available for different operating system or data structure.

(m) Tailor –made or 'customized' software will take time to write and will cost a lot more than standard software packages.

(n) An in-house tailor-made software development is only feasible for large organizations with a dedicated IT department.

Disadvantages of off-the-shelf packages

The disadvantages of application packages are as follows:

(a) The computer user gets a standardized solution to the task. A standard solution may not be well suited to the individual user's particular needs.

(b) The user is dependent on the supplier for maintenance of the package.

(c) They do not fit precisely the needs of the organization – the users may need to compromise what they want with what is available.

(d) The organization is dependent upon an outside supplier for the maintenance of the software.

(e) Different packages used by the organization may have incompatible data structures.

3.2.3 Advantages and disadvantages of bespoke systems

Advantages

(a) They are written to fit the organization's information needs precisely

(b) The system can be integrated with other applications within the organization.

(c) The system can be modified to fit changing need of the user over time.

(d) Bespoke systems might give a company a competitive advantage in the marketplace.

Disadvantages

(a) System development takes a long time, which delays the implementation of the system.

(b) Bespoke systems are costly to develop.

(c) There is a greater probability of bugs (software errors0 in a bespoke system.

(d) Support for a bespoke system will be expensive. The organization has to bear all the cost.

3.3 BUYING HARDWARE

In general terms, the choice of computer hardware will depend on the following factors:

(a) The ease with which the computer configuration fits in with the user's requirements (such as, direct access facilities, hard-copy output in given quantities).

(b) The processing speed, hard disk and storage size memory capacity of the system must be sufficient for current and foreseeable requirements and or be expandable.

(c) Reliability. The hardware should be durable and have a low breakdown rate. There should also be back-up facilities to minimize disruptions when the is down.

(d) Simplicity. Simple systems are bet for all organizations.

(e) Ease of communication between the hardware and the user.

(f) Scalability. The hardware should be able to meet new requirements as they emerge. Powerful CPUs tend to be more flexible and scalable.

(g) Security. Keeping out 'hacker's and other unauthorized users is easier with more powerful systems, although security can be a major problem for any computer system.

(h) Cost. The cost of the system should be reasonable

(i) Whether the choice of hardware will help with a smooth changeover from the old to the new system.

(j) Networking capacity

(k) Features to improve use of memory.

3.4 TRAINING

For an organization to get as much out of technology as it can, computer literacy must spread throughout all levels of the organization. Just as computerization will be impeded if systems are not user-friendly, so the successful adoption of IT will not happen if the organizational culture is not computer –friendly.

The issue of training becomes compelling in order to make personnel at all levels competent and willing to use IT. If management wishes to encourage end –user computing, then a training program must be part of the "IT revolution". Training is needed because if users are not adequately trained, they will not operate the system correctly or efficiently. Also, if users feel that they are being asked to perform tasks that are outside their capabilities, they may become demoralized and alienated.

Training is a key part of the implementation of a new system. The approach adopted and the medium through which training is given will vary depending on the target audience. Senior management are

more likely to be interested in the overall capabilities and limitations of the systems, while junior staff need to be taught the functional aspects.

Education is to be distinguished from training. The aim of education is to promote understanding and enhance awareness of the system. The focus of training however is skill building. Education has to do with providing staff with a general understanding of the system, the way it functions, it scope and it limitations. Training, in contrast, familiarizes the staff with the skills necessary to operate the computer system to perform specific tasks.

3.4.1 Types of Training

From the above, it should be clear that users need different types of systems training:

(a) Basic computer literacy and computer appreciation course, such as the concept of file updating and maintenance is needed.

(b) Users also need to learn how to use a particular application quickly, even if they do not go into the details of it. If the

system is complex, such training gives users an overall view of the system, commands and procedures.

(c) Users might sometimes need a refresher course, especially if they do not use a particular application regularly.

(d) Users need training while operating the application on the computer (on-the-job training)

The following are some of the ways to meet the above requirements:

(a) Traditional 'classroom' lectures

(b) Computer-based training involving on-screen practice on the computer

(c) In-house video production, involving interactive videos'

(d) Clear and comprehensive documentation and manuals for the system.

3.4.2 Levels of Training

Training must be designed to meet the specific needs of every level of staff. The following training groups can be particularly identified:

Operational staff: Operational staff are mainly responsible for recording transactions. Typically they will be entering amount into the system and taking telephone orders. Their tasks are routine, repetitive and limited. Their training will be targeted at the specific skills they need: such as how to enter a sale, or how to answer a customer query about product.

Tactical level: Staff at this level have some management tasks. Their jobs are more open-ended and their use of computers will have to be more flexible. Typically, they will need to know how to set up a spreadsheet and simple database.

Their training will be targeted at some specific skills but also at equipping them with more general skills. Staff at this level may be in a career structure and some training will equip them for their next jobs in the organization.

Strategic level: At this level, managers will be using management information system, decision support system and executive information system. They will need training in how to operate these. It is also likely that they would need some spreadsheet skills.

3.5 TESTING AND INSTALLATION

Importance of testing

After a system is developed, the stage is being gradually set for project implementation and eventual system completion. The system must however be tested before it can be confirmed ready for operation. Testing is an exhaustive and thorough process that determines whether the system turn out the desired conditions under known conditions. At this stage, the component is executed under specified conditions and the result are observed, recorded and evaluated.

Testing examines the system in order to ensure that all that needs to be built into it had been done to specification by assessing it for how it performs in a 'live' environment. In order to do this effectively, test data must be carefully prepared, results reviewed and corrections made, if necessary. Sometimes, the whole system or a part of it may be redesigned as a result of the test results. The benefit of testing is that it affords the opportunity to ascertain the behaviour of the system as well as execute and document under varying conditions.

It is essential that all aspects of testing be carefully considered and that they are as comprehensive as possible. To ensure this the development

team works with users to devise a systematic test plan. The test plan includes the preparations for the series of tests previously described. The plan is prepared by the development team in conjunction with the users. Testing an information system is of two types – system testing and user acceptance testing.

3.5.1 System testing

System testing examines the functioning of the information systems as a whole. System testing is usually carried out by the development team to ensure the technical completeness and functionality of the system. It tries to determine if discrete modules will function together as planned and whether discrepancies exists between the way the system actually works and the way it was conceived.

System testing will usually cover issues like:

(a) Interfaces between programs

(b) Suitability of input documents

(c) Practical input problems

(d) Availability of information when required

(e) Ability to modify data

(f) Performance time

(g) Performance time

(h) Procedures to deal with special situations

(i) Audit requirements

(j) Capacity for file storage and handling peak loads

(k) Durability of hardware

(l) Operating procedures and

(m) Recovery and restart capabilities

User acceptance testing

After the completion of systems testing, the system is passed on for user acceptance testing. In this stage, users or their representatives are asked to formally check whether the system fulfils their requirements. In practice, this is the time when deviations between the system operations and user's actual requirements become known.

Acceptance testing is conducted to determine whether or not a system satisfies its acceptance criteria and to enable the customer to determine whether or not to accept the system. It provides the final certification that the system is ready to be used in a production setting. Systems are evaluated by users and reviewed by management. When all parties

are satisfied that the new system meets their standards, the system is formally accepted for installation.

3.5.2 User acceptance testing will consider the functional characteristics of the system but is likely to repeat the detailed range and format checks undertaken in systems testing. User acceptance testing may also be concerned with:

(a) Testing and agreeing recurring activities such as month end routines.

(b) Testing and accepting generalized housekeeping functions (such as back up and restore).

3.5.3 End-User Participation

It is the end user, not the systems analyst, who must take overall responsibility for systems and who must decide whether to install a new system and operate the systems. The following definition of end-user is instructive.

'End users are the people that are required, or decide, to use directly the information systems in order to complete the tasks they have as part of their work or leisure activities.'

Users of information system vary considerably in level of skill they possess and in the tasks they perform. Users in a business environment may include clerk, accountants, programmers, secretaries as well as warehouse personnel, engineers, sales representatives and manages etc.

The end –user is a very important element in the successful acceptance of an information system. They are more likely to accept the system if they are involved extensively in the specification, development and use of the use of the system as well as its applications. In a system development process, end user involvement is especially important for the following reasons:

(a) Users understand the full range of data and processing conditions that may occur within their systems;

(b) Users can identify frequent and less common transactions, usually conditions to anticipate and most of the common types of errors that may occur when the system is in use; and

(c) Users can verify manual procedures more effectively.

3.6 FILE CREATION AND CONVERSION

Most commercial systems are file-based, depending on the processing of one or more files. These files must be created before the system is operational. If the new system involves the creation of new files such as computer files on a new medium, the system cannot become fully operational until the master files for the new system have been created. This process is known as file conversion. File conversion is the process of moving data from file in the existing system into files in the new system. These files could contain different information, and may be in a different format.

File conversion might be from a manual system to a computer system or from an existing computer system to a new computer system. This is a major part of systems implementation and must be fully controlled to ensure that errors are not allowed to creep into the new files. It is often an expensive part of the systems implementation because it usually means the conversion of existing manual file records into a medium used by the computer. Once the file has been created, extensive checking for accuracy is essential; otherwise considerable problems may arise when the system becomes operation.

It is the user department that carries the major workload here. Without careful planning, the result is always chaotic. This is the most crucial stage in the attainment of a new, successful system and in providing user confidence in it.

File conversion (or file creation) is always a major practical problem when a new computer-based system is being implemented. Some typical problems encountered in file conversion are:

Are source documents accurate and complete?

(a) Are the source documents up to date?

(b) Are the source documents in a form amenable to input into a program?

(c) Do different departments in the organization maintain compatible codes or descriptions for the same information?

(d) If different sections have conflicting data, then who is correct?

(e) What measure can be taken to ensure, as far as possible, that the converted file is free from input errors (such as keying –in-errors)?

Other problems of the conversion, which must be considered and planned by the system analyst, include the following:

(a) The possible provision of additional staff, or the use of a MIS consulting firm to cope with the file conversion and prevent bottlenecks.

(b) The establishment of cut-off dates where live files are to be converted (should the conversion be during slack time, for example, during holidays, weekends?)

(c) The decision as to whether files should be converted all at once, or whether the conversion should be file by file or record group by record group (with subsequent amalgamation).

3.6.1 PLANNING FILE CONVERSION

Planning a file conversion and controlling the work should proceed according to the following guidelines:

(a) Set a timetable for conversion; if possible try to do the conversion in a period when the volume of transactions is low.

(b) If possible, does a test run to see if all the information needed is available and that the input programs and the data validation routines are all working as planned?

(c) Decide upon a date after which no further information is to be held by the old methods, making sure that all subsequent data are held in a form suitable for transcription into the new system until the system is proved.

(d) Make sure that all relevant staff has been allocated enough time for training in the new system.

(e) As well as running the data validation programs, make continuous appraisal by means of output listings for the scrutiny of senior staff.

(f) Try to plan for the quickest possible changeover to the new system, giving the least disruption to users. Make sure all the key staff are available during the exercise and that disruption due to hardware failure has been properly assessed and covered.

(g) Authorize whatever overtime working is necessary to ensure that file conversion takes place according to the scheduled timetable.

In some situations, it may be desirable not to convert all the old files into the new system but to start afresh with the newly design computer system. This will usually entail the running of the old and new systems together for a period of time, until the old system can be phased out. Even in such cases, it is likely that certain data will still have to be extracted from the old files.

3.6.2 Conversion from manual record

Where the file conversion is from manual record the manager or system analyst in charge of planning the conversion must establish the following:

(a) The location of the data (data may be in one or more forms).

(b) Whether the existing forms are suitable for data capture.

(c) Whether the data format and sequence is suitable for the computer system.

(d) Whether the existing record is maintained centrally or not

(e) Whether the record is easily accessible.

(f) The volume involved

(g) Whether the existing files are to be converted directly or amalgamated in some way.

If the system is already computerized, the difficulties of file conversion will usually be reduced and the answer to the above problems more easily established. Furthermore, when it comes to the actual transcription from the old files to the new files, the use of a special conversion program will speed up the whole process.

3.6.3 Existing manual files

The stages in file conversion from manual files to computer files are normally as follows:

(a) Ensuring that the original record files are accurate and up to date.

(b) Recording the old file data on specially designed input documents will usually be done by the user department personnel following detailed instructions laid down by the system designer or software supplier. These instructions will include the procedures for allocating new code numbers and for checking the accuracy and

completeness of the data selected and entered on the input documents.

(c) Transcribing the completed input documents on to the new system may be done by user department staff keying in the data from the terminals.

(d) Using special programs to read the transcribed data and produce the required files in the appropriate form would include validation checks on the input data. The contents of the file must then be printed out and completely checked back to the data input forms (or even the original file if possible).

(e) Correcting any errors hat this checking reveals.

3.7 APPROACHES TO CHANGEOVER

Once standing data has been put on to files compatible with the new system, and the proposed system has been tested to the satisfaction of designers and users, the actual 'live'implementation of the system can begin. Once the system has been tested and files successfully converted, the system changeover can take place. the organization of the implementation effort may have to be interfaced with the ongoing

operations of the organization. The paramount thing is that management has full confidence in the new system before the changeover.

The initial operation of a new information system can be difficult tasks. This typically requires a conversion process from the use of a present system to the operation of a new or improved application. Conversion methods can soften the impact of introducing new information technologies into an organization. The nature of replaced operations and the nature of the new system may require one of the following approaches: direct changeover, parallel running, pilot tests and phased implementation. The four major forms of conversion are illustrated below:

3.7.1 DIRECT CHANGEOVER:

This is the method in which the old system is replaced by the new system in one move. It may be the only option where:

(a) The two- systems are significantly different and a complete change is the only practical way out.

(b) The former system is so ill structure that it is management decision to discontinue with it immediately.

(c) Some modules in the existing system are partially computerized while the new system is an integrated package.

Factors favouring the direct changeover method: Other factors that may favour the direct changeover method are:

(a) Where it is a small size system with low volume of data to be converted;

(b) Where an exceptionally qualified team is available to carry out conversion and implementation

(c) Where the new system is an integrated one that cannot be effectively implemented in phases

(d) Where there is a dependable fallback arrangement or workable alternative in the event of failure.

(e) Where it is difficult to handle transactions in parallel ; and

(f) Where there are demands from the user organization for immediate availability of the new system.

3.7.2 Advantages Of Direct Changeover Method

(a) The new system is immediately available and can be fully utilized.

(b) The cost saving can be very significant if no major problems occur; and

(c) It is relatively cost effective as resources are utilized on the new system while the old system is discontinued.

b. Disadvantages of Direct Changeover Method

a) It may disturb stability and order in the organization when users are learning and adapting to the new system.

b) The downside risks is high as in the event of failure, the whole process must be repeated with double disruptions of going back to the old system and changing again to the new.

c) Direct changeovers require a very brief period for transition. This may stretch the organization beyond its capacity, negatively impacting on the efficiency of business operations.

d) It requires scheduling for minimum workload period when all required personnel are available .

e) It is very risky as system or program corrections are difficult while the system has to continue running.

Direct changeovers should only be introduced during slack periods, holidays, or factory shutdown. This is because a minimum workload is required while users are adjusting to the new system.

3.7.3 PARALLEL RUNNING

Parallel running describes a method where the organization continues operations with both the old and the new system for some predetermined cycle. Within the cycle, the two systems are crosschecked before confidence is placed on the new system. It is therefore a cautious, safe and less risky approach.

There are two approaches to parallel running

Retrospective parallel running: This is an approach in which the new system operates on data already processed by the old system. For example, transactions already processed under the existing system may be input into the new system and reprocessed. Results from the parallel running may be checked against the existing results. The system is thereby assessed without the problems of staffing and disruption normally associated with parallel running.

Restricted parallel running: This is parallel running where the changeover is affected bit by bit. The approach is to run a complete logical part of the whole system as a unit in the new system. If the result of the piecemeal run is satisfactory, confidence in the new system is established and full-scale conversion of the remaining parts will follow.

Requirements for effective parallel running

The plan for parallel running must be well articulated and must include the following:

(a) A defined time limit or cycle on parallel running

(b) Effective error handling procedures

(c) Effective system-problem solving procedures and

(d) Determination of details and basis of crosschecks:

i. Input data –journal entries or output reports
ii. Full check or sample - depending on the importance attached to the data.
iii. Criteria for sample selection

The key requirements of parallel running are:

(a) The two systems have to be controlled
(b) Additional staff are required
(c) A long period is required for implementation.

The parallel running method is the most suitable option where the output of the old system need only be used for crosschecking and backup while actual operations utilize new system products.

Advantages of the parallel running method

(a) The parallel run period, when the two systems run concurrently, is a unique advantages of parallel running. The period creates opportunity for checking and is often described

as the 'period of bedding down'. During this period, hidden defects and problems are resolved and the efficiency of the system is brought up to a standard of normal running.

(b) A system that has been fully checked, corrected and perfected under actual operating conditions will be implemented.

(c) Failure of the new system will have less impact as normal processing can continue on the existing system.

(d) User personnel will have the time to become completely familiar with the new system.

(e) The output of both old and new systems will be available for comparison and evaluation.

Disadvantages of the parallel running method

(a) The direct costs can be very high as almost a complete duplication of processing is required

(b) The new and old organizational structures may be incompatible, thus foreclosing parallel running as a feasible option.

(c) The volume of work may be too large to be handled for two systems.

(d) The need for more staff and resources to cope with the two systems concurrently makes parallel running and expensive system.

(e) The duration of parallel run can vary considerably between systems – from two weeks to six months.

3.8 PHASE CHANGEOVER

This is a method where the changeover is carried out in time phases so that while the implementation is on, parts of the operations are handled under the old. It is best suited to very large projects and those where distinct parts of the system are geographically dispersed

it is most likely to be the only option for a large conglomerate with various subsidiaries and branches. This is particularly where the subsidiaries or branches are engaged in different activities or are subject to different regulations, statutory requirements, operating environments and seasonal fluctuations.

b. Factors favouring the phased changeover method

The critical factor in this method is control. This is because implementation is carried out in dispersed locations at different times. Control measures must be in place to ensure that the overall system remains totally synchronous. This is achieved by ensuring that systems amendments and improvements are incorporated in the later phases of the implementation.

Properly controlled and coordinated, this system has the potential of producing the best results as implementation can be improving progressively. On the other hand, failure can be costly and a poorly integrated system may result.

The factors favouring the phased changeover method are as follows:

(a) Where the system can be readily segmented into different phases, subsystems or geographical zones.

(b) Where the new and old organizations of the user establishment are structured that they can fit into the phasing arrangement.

(c) Where there are high demands on system reliability.

(d) Where the new system is a highly complex one that is difficult to implement at once or as unit.

Advantages of the phased changeover method

(a) The output of the implemented subsystems, phases and geographic zones are available for use while the implementation of the full system is ongoing.

(b) The risk of failure of a subsystem or phase is lower and recovery does not affect the whole system.

(c) User experience with a well designed and proven subsystem, phase or geographical zone will make the acceptance of the remaining parts of the system easier.

Disadvantages of the Phased Changeover Method

(a) The scheduling of cut-over of each phase, subsystem or geographic zone becomes very critical because for each phase, there is the alternative of immediate cut-over or parallel processing.

(b) The organization of the user departments and/or the nature of the system may not permit the division of the system into parts and implementing the system as such.

3.9 FORMULATING A STRATEGY AND DECIDING ON THE METHOD OF CHANGEOVER

When deciding on which method, or combination of methods, should be used for the changeover, management should consider the following:

(a) The strategy for coordinating the changeover and the persons responsible.

(b) The mechanism for complete and accurate communication for the whole system throughout the changeover period.

(c) The procedure for controlling errors and the measure of system change or program modification that can be allowed.

(d) The people affected by the change, how the change affects them and the identified training needs for their adaptation to the new system.

(e) The maintenance and operational methods of the new system.

(f) The method of monitoring and evaluating the result of the systems changeover.

Issues for Special Emphasis

(a) Timing is important. The new system should become operational at a time that is suitable to the user – especially when the workload is light, and not at a peak workload is light, and not at a peak workload time in the year.

(b) The conversion and implementation team must formulate a strategy for controlling the response to problems encountered during conversion and implementation.

SELF ASSESSMENT EXERCISE

- Highlight some of the issues that are involved in system testing.

4.0 CONCLUSION

In this unit, you have learnt about the nature and scope of system installation/implementation and maintenance. You have also been taught that training is a pivot upon which the success of system installation rotates. The unit has farther introduced you to file creation and conversion, planning file, conversion and approaches to changeover. The unit also discussed the advantages and disadvantages of the various methods of changeover employed.

5.0 SUMMARY

Acquisition and development of hardware, software and services end user training, testing and installation, system documentation file conversion and system change over form those activities that are involved in system installation/implementation and maintenance. One of the major advantage of off-the-shelf packages is that different packages will be available for different operating system or data structures. A defined time limit or cycle on parallel running makes up one of the requirements for effective parallel running.

When deciding on which method or combination of methods, should be used for the changeover , management should consider the strategy for coordinating the changeover and the persons responsible.

6.0 TUTOR MARKED ASSIGNMENT

* Enumerate some of the factors that are favourable to the phased changeover method.

Answer to Self Assessment Exercise

System testing will usually cover issue like

a. Inter faces between programs

b. Suitability of input documents

c. Practical input problems

d. Availability of information when required

e. Ability to modify data

f. Performance time etc.

7.0 REFERENCES/FURTHER READING

Charles T. Betz (2007): A Guide to Conceptual Data Models for it Managers.

Dan Farmer and Wiester Venema (2002): Forensic Computer Analysis: An Introduction Techweb.

Niv Ahitur and Seer Neumann (2004: Principles of Information Systems For Management", 3rd Edition, Nim C. Publishers

UNIT FOUR

CRITICAL FACTORS FOR THE SUCCESSFUL IMPLEMENTATION OF A MANAGEMENT INFORMATION SYSTEM

CONTENT

1.0 INTRODUCTION

Most failings in computerization are as a result of failing to plan. Adequate planning and adherence to professional standards should make it possible to progress toward system implementation with confidence.

Insoluble technical problems, cost overrun, time overrun, shortfalls in capacity, output deficiency, planning deficiencies, all form a wider spectrum of failures in computerization. System administration is responsible for coordinating the activities of the various functional areas and managing the utilization of the automated support areas and managing the utilization of the automated support system. The system administrator, usually very senior personnel in the establishment, is the person that is charged with the overall administration, and operation of a computer system. The systems development life cycle does not come to an end once a system has been implemented.

Common data problems are caused by; human error, poor documentation, physical computer fault, sabotage, poor training etc. Business systems involve – transaction processing system (TPS),

Production Support System, Executive Information Systems (EIS) Decision Support System (DSS) and the expert systems (ES).

2.0 OBJECTIVE OF THE UNIT

Upon successful completion of this unit, you are expected to do the following:

- Examine the critical factors responsible for the successful implementation of a management information system
- Discuss the defects in system administration
- Explain the concept of system maintenance and the relevant purposes.
- Discuss various project management techniques including traditional approach and the critical chain project management.
- Identify the various business systems and write short notes on each of them.
- Critically show the analysis of transaction processing and data back up procedures.
- Discuss the various data processing method.

3.1.0 CRITICAL FACTORS FOR THE SUCCESSFUL IMPLEMENTATION OF A MANAGEMENT INFORMATION SYSTEM

Most failings in computerization are as a result of failing to plan. Adequate planning and adherence to professional standards should make it possible to progress towards system implementation with confidence.

Failure in computerization can usually be traced to the following:

Insoluble technical problems

Computer systems may fail as a result of recurring technical problems that defy permanent solution. However, with advances in technology, this is becoming rare.

Cost overrun

Actual projects costs may exceed budgeted levels. The reasons for cost overruns vary and often result in the company's inability to recover initial capital investment. Computerization projects have been abandoned midway or commissioned as incomplete systems because of

cost overrun. The cost overrun may be as a result of abnormally high operating cost, which makes the system inefficient.

Time overrun

Projects are time-critical. Time overruns may arise either as a result delay in project takeoff or slow down in the planning process and implementation.

Shortfalls in Capacity

Project may not meet desired expectations due to underestimation of data volumes, patterns and over optimism about system performance. Planning failure usually result in the underperformance of the system.

Output deficiency

Reports are the primary system product. A system is regarded as failed when output (reports) from the system fails to meet the expectations.

Planning deficiencies

Most system failures can be traced to planning deficiency. Common failures due to flaws in planning are:

(a) failure in planning and choice of the option adopted;

(b) new systems are designed without a radical rethink of current operations;

(c) lack of underlying architecture or logical design

(d) user requirements are poorly defined

(e) resultant system is incomplete, lacking in relevant applications;

(f) system designers are unable to translate user requirements into technical requirements;

(g) computers are purchased on impulse rather than to satisfy information processing needs;

(h) systems are developed without planning the manual interfaces; and

(i) staffing is based on budgetary constraints and established personnel procedures, rather than on the skills needed to effective implementation computer applications.

3.2 DEFECTS IN SYSTEM ADMINISTRATION

System administration is responsible for coordinating the activities of the various functional areas and managing the utilization of the automated support system. The System Administrator, usually very

senior personnel in the establishment, is the person that is charged with the overall administration, and operation of a computer system. It is the responsibility of the system administrator to coordinate all aspects of the system and ensure that they work together to achieve the objectives of the system development.

Common defects in system administration are:

(a) Inability to control technology and adjust to software updates

(b) Inability to react quickly to new developments

(c) Concentration of responsibilities in only few individuals

(d) Access to the system by unauthorized users

(e) Misuse of the system by authorized users

(f) Poor quality control of system operations; and

(g) Data management problems – incorrect entry of data, erroneous or falsified input.

3.2.1 Failings in management oversight

It is the responsibility of top management to keep an eye on the entire operation and keep the system on track. Failings in management oversight are usually as a result of:

(a) Organization structure has not been realigned to complement the demands of computerization

(b) Failure to manage data as an organizational resources

(c) Inadequate assignment of responsibilities to cope with work reinvention and re- systematization.

(d) Lack of effective communication

(e) Failure to development the necessary skills in operating staff;

(f) Hiring the wrong people

(g) Failure to provide staff with additional training necessary to develop or improve skills

(h) Employment of wrong measures in evaluating staff performance; and

(i) Inadequate technical training for users.

3.2.2 Poor system implementation

Failure usually occur during system implementation as a result of inability to interpret and implement user requirements correctly or failure to provide adequate controls.

3.2.3 Critical factors for successful IT project implementation

From the above, the following factors are critical for successful system implementations:

(a) Well-defined mission, purpose and objective;

(b) Proper scheduling and planning;

(c) User involvement, consultation with operators and effective communication among all concerned. Users must be involved full time, throughout the project.

(d) Appropriate personnel –in skills, number, knowledge and exposure;

(e) Up to date technical skills and technology

(f) End user/client acceptance

(g) Monitoring and feedback and

(h) Visible top management support

3.3 SYSTEM MAINTENANCE

The systems development life cycle does not come to an end once a system has been implemented. There will inevitably be some error in the system after it has been implemented. There will also be, over a period of time, changes to activities and procedures in the 'real world', and so systems functions and processes may need to be modified

accordingly. Throughout its life, for a system to operate effectively and efficiently, it must be maintained.

The term maintenance is normally used to describe the process of modifying a system after it has been implemented and is in use, to correct errors and provide new facilities. It is the re-execution of earlier stages of the development process for certain parts of the system in order to correct some errors after the system has been implemented. It is the modification of systems functions and processes in order to cope with changes in the operating environment. Maintenance enables the system to function as designed or bring it to a new state of operations and capability.

3.3.1 Purpose of system maintenance

This system will also need to be reviewed and maintained periodically for the following reasons:

(a) To deal with unforeseen problems arising in operation, such as, programmes requiring to be modified to deal with unforeseen circumstances.

(b) To confirm that the planned objectives are being met and to take action if they are not.

(c) To ensure that the system is able to cope with the changing requirements of business.

When considering the causes of system maintenance, there is a need to differentiate between the immediate spur to the maintenance activity and the underlying causes. It is important for systems designers to build in mechanism that identify when maintenance is needed, and to start the process of updating the system.

Both the underlying causes of maintenance and the immediate spurs will vary according to the type of maintenance being undertaken, each type of maintenance needs to be examined separately.

There are three types of maintenance activity: corrective maintenance, perfective maintenance and adaptive maintenance. Corrective maintenance is carried out following a systems failure, perfective maintenance aims to make enhancements to systems while adaptive maintenance takes account of anticipated changes in the processing environment. System maintenance is usually necessitated by the

presence of errors, by changes in user requirements or by the existence of poor documentation.

3.3.2 Corrective maintenance

Corrective maintenance usually consist of action in response to a problem.

The basic underlying cause of corrective maintenance is a system failure. This may be an error in one of the programs, or it may be that data has become corrupted. Program bugs are likely to be caused by ineffective testing or by the failure to undertake adaptive maintenance when required.

Data problems are caused by:

(a) Human error

(b) Poor documentation

(c) Physical computer faults

(d) Sabotage

(e) Poor training

(f) Inadequate supervision

(g) Unforeseen impact of other computer systems ;

(h) Malicious damage caused to both programs and data.

Corrective maintenance is carried out when there is a systems failure, for example in processing or in an implementation procedure. This is the type of maintenance which many people think of when they think of maintenance. Its objective is to ensure that systems remain operational. It is carried out to correct faults in hardware or software. Corrective maintenance is reactive and is usually carried out as a result of a negative experience with the system. It often consist of action in response to a problem or reaction to an event.

3.3.3 Perfect maintenance

Perfect maintenance is carried out in order to perfect the software, or to improve software so that the processing d inefficiencies are eliminated and performance is enhanced. Much perfective maintenance consists of making enhancements requested by users to improve or extend the facilities available. The user interface may be amended to make software more user-friendly. The replacement of a word processing package written for Windows 3.1 by a package which works in a windows 95 environment is an example of perfective maintenance.

Perfective maintenance is carried out to improve the performance, maintainability, overall effectiveness or other attributes of a system. It may be prompted by the availability of new technology, the development of new techniques, or by a request for system enhancement from the users. Its essence is to make the software better or to improve it so that processing inefficiencies are eliminated and performance is enhanced. Perfective maintenance involves making enhancements requested by users to improve and extend the facilities available to it.

3.3.4 Adaptive Maintenance

Adaptive maintenance is carried out to take account of anticipated changes in the processing environment. For example, new taxation legislation might require change to be made to payroll software.

There are three basic reasons why adaptive maintenance may be needed:

(a) User requirements may have changed or have been ill defined when the system was being designed.

(b) The system environment may have significantly changed

(c) The system may have grown beyond the limits that were originally envisaged for it.

Adaptive maintenance enables a system to adjust to changes in its environment. User information needs may change; organizations structure may be altered; legislative changes may impose new obligations on the software. Adaptive maintenance is carried out to take account of anticipated changes in the processing environment. Changes in users operating procedures occur from time to time and software may require amendment to reflect this. Changes in legislation can lead to a need for amendment to software, for example, new taxation legislation might require change to be made to payroll software. A hardware upgrade might require an adaptation of software or even complete reprogramming.

3.3.5 Preventive Maintenance

Preventive maintenance is maintenance carried out in advance of a problem occurring. It is the same as having a car regularly serviced in order to reduce the risk of breakdowns. In theory, more preventive maintenance means less corrective maintenance. This is good, because preventive maintenance can be carried out at a time most convenient

to the organization, whereas corrective maintenance always seems to be required during the busiest periods.

3.4 PROJECT MANAGEMENT TECHNIQUES

Project management is the process of planning, organizing and managing resources to bring about the successful completion of specific project goals and objectives.

A project is a definite endeavor (having specific start and completion dates) undertaken to create a unique product or service which brings about beneficial change or added value. This characteristics of projects standards in sharp contrast to processes, or operations, which are permanent or semi-permanent functional work to repetitively produce the same product or service. In practice, the management of these two systems is often found to be quite different, and as such requires the development of distinct technical skills and the adoption of separate management.

The primary challenge of project management is to achieve all of the project goals and objectives while honouring the project constraints. Typical constraints are scope, time and budget. The secondary –and

more ambitious –challenge is to optimize the allocation and integration of inputs necessary to meet predefined objectives.

There are several approaches that can be taken to managing project activities including agile, interactive, incremental, and phased approaches. Regardless of the approach employed, careful consideration needs to be given to clarify surrounding project objectives, goals, and importantly, the roles and responsibilities of all participants and stakeholders.

3.4.1 The traditional approach

A traditional phased approach identifies a sequence of steps to be completed. In the 'traditional approach", we can distinguish 5 components of a project in the development of a project:

a) Project initiation stages

b) Project planning or design stage

c) Project execution or production stage

d) Project monitoring and controlling systems

e) Project completion stage

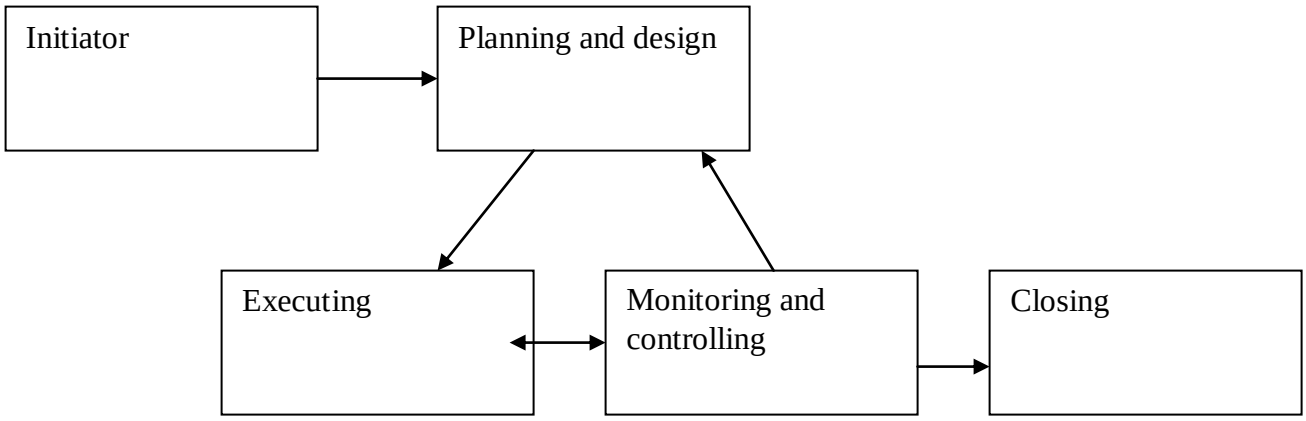


Figure 3.4: Typical development phases of a project

Not all the projects will visit every stage as project can be terminated before they reach completion. Some projects probably do not have the planning and/ or the monitoring stage. Some projects will go through steps 2, 3 and 4 multiple times.

Many industries utilizes variation on these stages. For example, in software development, this approach is often known as "waterfall development" , i.e. one series of tasks after another in linear sequence. Waterfall development can work for small tightly defined projects, but for larger projects of undefined or unknowable scope, it is less suited. Because software development is often the realization of a new or novel product which is often surrounded by a cloud of

uncertainties, this method has been widely accepted as ineffective for software projects where requirements are largely unknowable up front and susceptible to change. While the names may differ from industry to industry, the actual stages typically follow common steps to problem solving– 'defining the problem, weighting options, choosing a path, implementation and evaluation."

3.4.2 Critical chain project management

Critical chain project management (CCPM) is a method of planning and managing projects that puts more emphasis on the resources required to execute project tasks. It is an application of the Theory of Constraints (TOC) to projects. The goal is to increase the rate of throughout (or completion rates) of projects in an organization. Applying the first three of the five focusing steps of TOC, the system constraint for all projects is identified as resources. To exploit the constraint, tasks on the critical chain are given priority over all other activities. Finally, projects are planned and managed to ensure that the critical chain tasks are ready to start as soon as the needed resources are available, subordinating all other resources to the critical chain.

For specific projects, the project plan should undergo Resource Leveling, and the longest sequence of resource- constrained tasks is

identified as the critical chain. In multi-project environments, resource leveling should be performed across projects. However, it is often enough to identify (or simple select) as single 'drum' resource- a resources that acts as a constraint across projects – and stagger projects based on the availability of that single resource.

3.4.3 Extreme project management

In critical studies of project management, it has been noted that several of these fundamentally PERT-based models are not well suited for the multi-project company environment of today. Most of them are aimed at very large-scale, one-time, one-routine projects, and nowadays all kinds of management are expressed in terms of projects.

Using complex models for "projects" (or rather "tasks") spanning of few weeks has been proven to cause unnecessary costs and low maneuverability in several cases. Instead, project management experts try to identify different "lightweight" models, such as Agile Project Management methods including Extreme Programming for software development.

The generalization of Extreme Programming to other kinds of project is extreme project management, which may be used in combination with

the process modeling and management principles of human interaction management.

3.4.4 Event chain methodology

Event chain methodology is the next advance stages beyond critical path method and critical chain project management,. Event chain methodology is an uncertainty modeling and schedule network analysis technique that is focused on identifying and managing events and event chains that affect project schedules. Event chain methodology helps to mitigate the negative impact of psychological heuristics and biases, as well as to allow for easy modeling of uncertainties in the project schedules. Event chain methodology is based on the following major principles.

(a) Probabilistic moment of risk: An activity (tasks) in most real life processes is not a continuous uniform process. Tasks are affected external events, which can occur at some point in the middle of the task.

(b) Event chains: Event can cause other events, which will create event chains. These event chains can significantly affect the course of the project. Quantitative analysis is used to

determine a cumulative effect of these event chains on the project schedule.

(c) Critical events or event chains: The single events or the event chains that have the most potential to affect the projects are the “critical events” or “critical chains of event.” They can be determined by the analysis.

(d) Project tracking with events: If a project is partially completed and data about the project duration, cost and events occurred is available, it is possible to refine information about future potential events and helps to forecast future project performance.

(e) Event chain visualization: Events and event chains can be visualized using event chain diagrams on a Gantt chart.

3.4.5 The PRINCE 2 Process Model

PRINCE2 is a structured approach to project management, released in 1996 as a generic project management method. It provides a method for managing projects within a clearly defined framework. PRINCE2 describes procedures to coordinate people and activities in a project,

how to design and supervise the project and what to do if the project has to be adjust if it doesn't develop as planning.

In the method each process is specified with its key inputs and outputs and with specific goals and activities to be carried out, which gives and automatic control of any deviations from the plan. Divided into manageable stages, the method enables an efficient control of resources. On the basis of close monitoring the project can be carried out in a controlled and organized way. PRINCE2 provides a common language for all participants in the project. The various management roles and responsibilities involved in a project are fully described and are adaptable to suit the complexity of the project and skills of the organization.

3.4.6 Rational unified process

The Rational Unified Process (RUP) is an iterative software development process framework created by the Rational Software Corporation, a division of IBM since 2003. RUP is not a single concrete prescriptive process, but rather an adaptable process framework, intended to be tailored by the development organizations and software project teams that will select the elements of the process that are appropriate for their needs. The following are phases of RUP, which align to business

activities intended to drive successful delivery and deployments of projects:

(a) Inception – Identify the initial scope of the project, a potential architecture for the system, and obtain initial project funding and stakeholders acceptance.

(b) Elaboration – Prove the architecture of the system

(c) Construction – Building working software on a regular, incremental basis which meets the highest-priority needs of project stakeholders.

(d) Transition – validate and deploy the system into the production environment.

3.5 BUSINESS SYSTEMS

3.5.1 Transaction Processing System (TPS)

A transaction processing system is an information system that performs the recording and processing daily routine transactions generated through the occurrence of business activities. They are used for routine tasks in which data items or transactions must be processed

so that operations can continue. Examples of the application of TPS include handling of sales orders, purchase orders, payroll items and stock records

A transactions processing system provides the raw materials, which often used more extensively by a management information system, database or decision support systems. In other words, a transactions processing system might be used to produce management information, such as reports on cumulative sales figures to date, total amounts owed to suppliers or owed by debtors, total stock turnover to date and value of current stock-in-hand. The main purpose of a TPS is to handle day-to-day business operations and it represent the lowest level in an organization's use of information system. Data generated from a typical TPS form the input to other information systems.

Transactions processing systems are widely used in organization with high volume of transactions resulting in benefit such as efficiency of operations, fast turnarounds, answers to enquiries, reduction in inventory and staff saving. It has to be noted, however, that transactions processing systems are most suited for high volume transactions with predefined tasks, decision rules and transaction flows.

3.5.2 Production support systems

A production support system is an information system that provides an innovative and automated approach to production processes. It ranges from using modern software to design new products to automated monitoring and optimizing production processes and devices. Today, there are 3-Dimension computer –aided design (CAD) and collaborative product development system s that are used for product design and convey the product information for manufacturing. This include data such as geometric dimensioning and tolerancing, 3D annotation (text) and dimensions, surface finish and material specifications.

There is also computer-aided manufacturing (CAM) which uses computer-based software tools that assist engineers and machinists in manufacturing or prototyping product components. CAM is a programming tool that makes it possible to manufacture physical models using computer-aided design (CAD) programs. CAM creates real life versions components designed within a software package. CAM was first used in 1981 for car body design and tooling.

3.5.3 Executive Information System (EIS)

Executive information system is an information system that provides strategic information tailored to the needs of executives, top management information system for helping managers to identify and address problems and opportunities. This it does by collecting, analyzing and presenting data in a format that is easy to use by top executives and providing selected and summarized information for them. This way, an executive information system (EIS) provides the executive with the underlying performance facts and figures that have traditionally been under the control of middle managers.

The first goal of an executive information system is to provide top executive with immediate and easy access to information about a company's critical success factors (CSFs), that is, key factors that are critical to accomplishing an organization's strategic objectives. A great advantage of executive information systems is in giving the executive easy access to key internal and external data. They typically include a 'drill-down' facility, graphic and data manipulation facilities for rapid and simple retrieval of the require data. They assist top management by providing information on critical areas of the organization's activities drawn from both internal and external databases.

An EIS is likely to have the following features:

(a) Provision of summary – level data, captured from the organization's main systems.

(b) A facility which allows the executive to 'drill-down' from higher levels of information to lower levels.

(c) Data manipulation facilities, for example, comparison with budget or prior year data.

(d) Graphic, for user-friendly presentation of data.

(e) A template system. This will mean that the type of data (e.g. sales figures) is presented in the same format, irrespective of changes in the volume of information required.

The basic design philosophy of executive information system is as follows:

(a) It should be easy to use.

(b) It should make data easy to manipulate so that it presents information in the executive's point of view.

(c) It should provide tools for analysis such as ratio analysis, forecast, what –if analysis and trends.

(d) It should provide aids for presenting information in narrative numeric, graphic, colour and other forms.

a. Decision Support System (DSS)

A decision support system is an information system at the management level of an organization that combines data, analytical tools, and models to support semi-structured and unstructured decision making. These system use data collected by transaction –processing systems to evaluate business models and assist managers in making tactical decisions. There are three major mechanisms – data collection, analysis of models, and presentation.

A decision support system is used by management to assist in making unstructured decisions on issues that do not allow the easy application of many of the techniques or systems develop for well-defined problems or activities. Unstructured decisions are decisions which must be made in situations where it is not possible to specify in advance most of the decision procedures to follow; where there may be several "right" answers, and no precise way to get a right answer.

A decision support system is intended to provide a wide range of alternative information gathering and analytical tools with a major emphasis upon flexibility and user-friendliness. A decision support system does not make decisions. The objective is to allow the manager to consider a number of alternatives and evaluate them under a variety of potential conditions. It is operated by the end user and exists to supplement human judgment in semi-structured decision-making. Managers using this system often develop scenarios using earlier results to refine their understanding of the problem and their actions. A decision support package include: modeling, spreadsheets, forecasting, linear programming, statistical analysis, expert systems and so on.

The benefits of a DSS are:

(a) The computer provides support but neither replace the manager's judgment nor provides predetermined solutions.

(b) DSS is best suited to semi-structured problems where parts of the analysis can be computerized but the decision maker's judgment and insight is needed to control the process.

(c) A DSS provides a platform where effective problem solving is enhanced by interaction between the computer and the manager .

b. Expert Systems (ES)

An expert system is a form of decision support system that allows users to benefit from expert knowledge and information. It is a computer-based application that attempts to incorporate as much knowledge of a particular discipline in a database as is held by expert practitioners and theorists in the field. Their function is to implement heuristic (unstructured) approaches to solving problems within the subject area by drawing inferences from a knowledge base acquired by human expertise. An expert system is a form of DSS that allows users to benefit from expert knowledge and information.

An expert system assist with decision –making, where the process of analyzing the problem calls for the application of logical reasoning rather than computation work. This way, it provides help for 'experts' in making an analysis and reaching a judgment. An example of an expert system is a medical computer system that can be used to analyze the symptoms of a patient's condition and to assist with reaching a medical diagnosis. Another examples is a legal expert that

can be used by solicitors to analyse a case, and reach a view on how the cases should be handled on behalf of the client. The system will consist of a database holding specialized data and rules about what to do in, or how to interpret, a given set of circumstances.

An expert system uses artificial intelligence, that is, the concept that computers can be programmed to imitate certain features of human reasoning. It can be used where problems are reasonably well defined and can be solved by reference to a set of rules. An organization can use an expert system when a number of condition are met.

(a) The problem is reasonably well defined

(b) The expert can define some rules by which the problem can be solved

(c) The problem cannot be solved by conventional transaction processing or data handling

(d) The investment in an expert system is cost-justified

For example, many financial institution now use expert system to process straightforward loan applications. The user enters certain key facts into the system such as the loan application's name and most recent addresses, their income and monthly outgoing, and details of other loans. They system will then:

(a) Check the facts given against its database to see whether the applicant has a good previous credit record.

(b) Perform calculations to see whether the applicant can afford to replay the loan; and

(c) Match other criteria, such as whether the security offered for the loan or the purpose for which the loan is wanted is acceptable, and to what extent the loan applicant fits the lender's profile of a good risk (based on the lender's previous experience).

c. Artificial Neural Networks (ANN)

Artificial neural networks are made up of interconnecting artificial neurons (i.e. programming constructs that mimic the properties of biological neurons). Artificial neural networks may either be used to gain and understanding of biological neural networks, or for solving artificial intelligence problem without necessarily creating a model of a real biological system. The real, biological nervous system is highly complex and include some features that may seem superfluous based on an understanding of artificial networks.

ANN try to simulate some properties of neural networks by aiming at building mathematical models of biological neural systems. Neural networks have been applied successfully to speech recognition, image analysis and adaptive control, in order to construct software agents (in computer and video games) or autonomous robots. Most of the currently employed artificial neural networks for artificial intelligence are based on statistical estimation, optimization and control theory.

3.6 TRANSACTION PROCESSING

Phases of transaction processing systems:

i. Data entry/capture

This refers to the process of entering data into a computer system, which can be manual process where data is entered through a keyboard, or by scanner, or other equipment, or may be automatic where a system is receiving a transmission from another program or computer.

ii. Data transmission

Data transmission is the physical transfer of data over a point-to-point or point-to-multipoint communication channel. Examples of such channels are copper wires, optical fibers, wireless communication channels, and storage media. The data is often represented as an electromagnetic signal, such an electrical voltage signal, radio wave or microwave signal or an infra-red signal.

Data transmitted may be a digital bit stream originating from a data source, for example a computer or a keyboard. It may also be an analog signal such as a phone call or a video signal, converted or digitized into a bit-stream for example using pulse-code modulation (PCM) or more advanced source coding (data compression) schemes. This source coding and decoding is carried out by coded equipment.

1. File look-ups, calculations, logical comparisons

File/Data Look-Ups

During data entry, some application software provides file/data look-ups on some key fields or data item. This is usually a popup menu that displays, either automatically or by tapping a key, of a list of options a

user must select from. This serves to control and maintain a uniform data for that particular data item which eventually support query of data for ad hoc information request.

Example of this is where a data entry in a transaction processing demands capturing customer's state of origin, it might be necessary for a list of states available to popup so that data entry operator can look it up and make a selection instead of having a type of it every time. This help to reduce entry time and guarantee data consistency.

Logical comparisons

In entering or capturing data, some data items are compared logically with a predefined data values as a control to ensure an entry fall within a predefined range. If the entered value falls below or above the range, an error message may be displayed to alert the data entry operators so as to make the necessary correction.

2. Master file updates

Master file update is the process of updating the content of a master file with new transaction entries. This update is usually done at predefined frequency depending on the type of transactions involved

or could be determined by the frequency of information request that depends on the master file. This frequency of mater file update is usually part of the operational procedures in any transaction processing system.

Usually, there are several types of files involved in a typical data processing system. There is the transaction file which stores day-to-day transaction entries like daily sales entry. Secondly, there could be intermediate files and then thirdly the master files. The intermediate and master files must be updated with the summarized data from the transaction file at a predefined period interval for information currency.

3. Storage, Record Retention, Back-up

Data storage

Storage of data in computer is a very crucial issue that computer users cannot joke with. In fact, as part of being computer literate, one must be proficient in the area of data file storage in the computer system. Ignorance of this may be very costly for a computer user. Computer stores data in the following storage media. In any of these, data is stored in an inverted tree-like-structure.

Magnetic tape

Magnetic tape has for long been the most commonly used medium for bulk data storage, backup, archiving and interchange. Tape has typically had an order of magnitude better capacity/price ratio when compared to hard disk, but recently the ratios for tape and hard disk have become a lot closer. There are myriad formats, many of which are proprietary or specific to certain markets like mainframes or a particular brand of personal computer. Tape is a sequential access medium, so even though access time may be poor, the rate of continuously writing or reading data can actually be very fast. Some new tape drives are even faster than modern hard disks.

Hard disk

The capacity/ price ration of hard disk has been rapidly improving for many years. This is making it more competitive with magnetic tape as a bulk storage medium. The main advantages of hard disk storage are low access times, availability, capacity and ease of use. External disks can be connected via local interfaces like SCSI, USB or FireWire, or via longer distance technologies like Ethernet, iSCSI, or Fibre Channel.

Optical disc (or Compact Disc – CD)

A recordable CD be used as a backup device. One advantage of CDs is that they can be restored on any machine with a CD-ROM drive. In addition, recorded CD's are relatively cheap. Another common format is recordable DVD.

Floppy disk

During the 1980s and early 1990s, many personal/home computer users associated backup mostly with copying floppy into disks. The low data capacity of a floppy disk makes it an unpopular and obsolete choice today.

Solid state storage

Also known as flash memory, thumb drives, USB flash drives, CompactFlash, SmartMedia, Memory Stick, secure Digital cards, etc. these devices are relatively cost for their low capacity, but offer excellent portability and ease –of-use.

Remote backup service

As broadband internet access becomes more widespread, remote backup services are gaining in popularity. Backing up via the internet to a remote location can protect against some worst-case scenarios such as fires, floods, or earthquakes which would destroy any backups in the immediate vicinity along with everything else. A drawback to a remote backup service is that an internet connection is usually substantially slower than the speed of local data storage devices, so this can be a problem for people with large amounts of data. It also has the risk associated with putting control of personal or sensitive data in the hands of a third party.

3.7 DATA BACKUP PROCEDURE

Backup refers to making copies of data so that these additional copies may be used to restore the original after a data loss event. These additional copies are typically called 'backups'. Backups are useful primarily for two purposes. The first is to restore a state following a disaster (called disaster recovery). The second is to restore small numbers of files after they have been accidentally deleted or corrupted. Backups are typically that last line of defense against data loss, and consequently the least granular and the least convenient to use.

Since a backup system contains at leas one copy of all data worth saving, the data storage requirements are considerable. Organizing this storage space and managing the backup process is a complicated undertaking which must be planned as an integral part of an information control or security management process.

Many different techniques have been developed to optimize the backup procedure. These include following:

Snapshot backup

A snapshot is an instantaneous function of some storage systems that present a copy of the file system as if it was frozen in a specific point in time, often by a copy –or-write mechanism. And effective way to backup live data is to temporarily freeze it (e.g. close all files), take a snapshot, and then resume live operations. At this point the snapshot can be backed up through normal methods. While a snapshot is very handy for viewing a filesystem as it was at a different point in time, it is hardly an effective backup mechanism by itself

Open file backup

Many backup software packages feature the ability to handle open files in backup operations. Some simply check for openness and try again later. When attempting to understand the logistics of backing up open files, one must consider that the backup process could take several minutes to backup a large file such as a database. In order to backup a file that is in use, it is vital that the entire backup represent a single-moment snapshot of the file, rather than a simple copy of a red-through. This represents a challenge when backing up a file that is constantly changing. Either the database file must be locked to prevent changes, or a method must be implemented to ensure that the original snapshot is preserved long enough to be copied, all while changes are being preserved.

Cold database backup

During a cold backup, the database is closed or locked and not available to users. The data files do not change during the backup process so the database is in a consistent state when it is returned to normal operation.

Hot database backup

Some database management systems offer a means to generate a backup image of the database while it is online and usable ("hot"). This usually includes a consistent image of the data files plus a log of changes made while the procedure is running. Upon a restore, the changes in the log files are reapplied to bring the database in sync.

Accounting, control, management and reporting

To minimize errors, disaster, computer crime and breaches of security, special policies and procedures must be incorporated into the design, implementation and continual usage of information system. The combination of manual and automated measures that safeguard information system and ensure performance according to management standard is termed controls. Controls consist of all the methods, policies and organizational procedures that ensure the safety of the organizations' assets, the accuracy and reliability of its accounting records and operational adherence to management standards

In the past, the control of information systems was treated as an afterthought addressed only toward the end of implementation just before the system was installed. Today, however, organizations are so

critically dependent on information systems that vulnerabilities and control issues must be identified as early as possible. The control of an information system must be an integral part of it design. Users and builders of systems must pay close attention to control throughout the system's life span.

Computer system are controlled by a combination of general controls and application controls. General controls are those that control the design, security, and use of computer programs and the security of data files in general throughout the organization. On the whole, general controls apply to all computerized application and consist of a combination of system software and manual procedures that create and overall control environment.

Query, audit trail, ad-hoc reports

Query

This is a database management system feature that provides for extracting information from a database through a structured language called structured query language, or SQL. This language contains commands that permit end users and programming specialists to

extract data from the database to satisfy information requests and develop applications. Examples of query statement is provided below:

Example:

(a) SELECT * FROM salesman

(b) SELECT fname, Iname, EmpID, doBirth

FROM employees WHERE empID = 34554

Error prevention, detection, correction

In data capturing, error detection and correction has great practical importance in maintaining data (information) integrity across storage media.

Definition of error detection and error correction:

(a) Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver.

(b) Error correction is the additional ability to reconstruct the original, error-free data.

There are two basic ways to design the channel code and protocol for an error correcting system:

(a) Automatic repeat-request (ARQ): The transmitter sends the data and also an error detection code, which the receiver uses to check for errors, and request retransmission of erroneous data. In many cases, the request is implicit; the receiver sends an acknowledgement (ACK) of correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time.

(b) Forward error correction (FEC): The transmitter encodes the data with an error-correcting code (ECC) and send the coded message. The receiver never sends any messages back to the transmitter. The receiver decodes what it receives as the 'most likely' data. The codes are designed so that it would take an 'unreasonable' amount of distortions to trick the receiver into misinterpreting the data.

It is possible to combine the two, so that minor errors are corrected without retransmission and major error are detected and a retransmission requested. The combination is called hybrid automatic repeat-request.

Error detection scheme

Several schemes exist to achieve error detection, and generally they are quite simple. All error detection codes (which include all error-detection- and –correction code) transmit more bits than were in the original data.

Most codes are “systematic”: the transmitter sends a fixed number of original data bits, followed by fixed number of check bits (usually referred to as redundancy in the literature) which are derived from the data bits by some deterministic algorithm. The receiver applies the same algorithm to the received data bits and compare its output to the received check bits; if the values do not match, an error has occurred at some point during the transmission.

Repetition scheme: Variations on this scheme exist. Given a stream of data that is to be sent, the data is broken up into blocks of bits, and in sending, each block is sent some predetermined number of times. For example, if we want to send “1011”, we may repeat this block three times each. Suppose we send “1011 1011 1011”, and this is received as “1010 1011 1011”. As one group is not the same as the other two, we can determine that an error has occurred. This scheme is not very efficient, and can be susceptible to problems if the error occurs in

exactly the same place for each group (e.g. “1010 1010 1010” in the example above will be detected as corrected in this scheme). The scheme however is extremely simple, and is in fact used in some transmissions of number.

Parity schemes: A parity bit is an error detection mechanism that can only detect an odd number of errors. The stream of data is broken up into blocks of bits, and the number of 1 but is counted. Then a “parity bit” is set (or cleared) if the number of one bits is odd (or even). (This scheme is called even parity; odd parity can also be used). If the tested blocks overlap, then the parity bits can be used to isolate the error, and even correct it if the error affects a single bit: this is the principle behind the Hamming code. There is a limitation to parity scheme. A parity bit is only guaranteed to detect an odd number of bit errors (one, three, five and so on). If an even number of bits (two, four, six and so on) are flipped, the parity bit appears to be correct, even though the data is corrupt.

Checksum: A checksum of a message is an arithmetic sum of message code words of a certain word length, for example byte values, and their carry value. The sum is negated by means of one-complement, (1’s) and stored or transferred as an extra code word extending the message.

On the receiver side, a new checksum may be calculated from the extended message. If the new checksum is not 0, an error has been detected. Checksum schemes include parity bits, check digit, and longitudinal redundancy check.

Cyclic redundancy checks: More complex error detection (and correction) methods make use of the properties of finite files and polynomials over such fields. The cyclic redundancy check considers a block of data as the coefficients to a polynomial and then divides by a fixed, predetermined polynomial. The coefficients of the result of the division is taken as the redundant data bits, the CRC.

On reception, one can recomputed the CRC from the payload bits and compare this with the CRC that was received. A mismatch indicates that an error occurred

Hamming distance based checks: If we want to detect 'd' bit errors in an 'n' bit word we can map every 'n' bit word into a bigger 'n+d+1' bit word sot that the minimum hamming distance between each valid mapping is 'd+1. This way, if one receives a 'n+d+1' word that does not match any word in the mapping (with a hamming distance 'x <=d+1= from any word in the mapping) it can successfully detect it as an erroneous words. Even more, 'd' or fewer errors will never transform a valid word

into another, because the hamming distance between each valid word is at least 'd+1', and such errors only lead to invalid words that are detected correctly. Given a stream of 'm*n'bits, we can detect 'x<=d' bit errors successfully using the above method on every n bit word. In fact, we can detect a maximum of 'm*d' errors if every n word is transmitted with maximum d errors.

Horizontal and vertical redundancy check: Other types of redundancy check include horizontal redundancy check, vertical redundancy check and "double", "dual" or "diagonal" parity.

Polarity schemes: One less commonly used form of error correction and detection is transmitting a polarity reversed bit stream simultaneously with the bitstream it is meant to correct. This scheme is very weak at detecting bit errors, and marginally useful for byte or word error detection and correction.

Error correction

Automatic repeat request: automatic repeat re-Quest (ARQ) is an error control method for data transmission which makes use of error detection codes, acknowledgement and/or negative acknowledgement messages and timeouts to achieve reliable data transmission. An

acknowledgement is a message sent by the receiver to the transmitter to indicate that it has correctly received a data frame.

Usually, when the transmitter does not receive the acknowledgement before the timeout occurs (i.e. within a reasonable amount of time after sending the data frame), it retransmits the frame until it is either correctly received or the error persists beyond a predetermined number of retransmissions. A few types of ARQ protocols are Stop- and-wait ARQ. Go back-N ARO and Selective Repeat ARQ. Hybrid ARQ is a combination of ARQ and forward error correction.

Error –correcting code: An error-correcting code (ECC) or forward error correction (FEC) code is a code in which each data signal conforms to specific rules of construction such that departures from that construction in the received signal can be automatically detected and corrected. Error-correcting codes are used in computer data storage, for example in dynamic RAM, and in data transmission.

The basic strategy is for the transmitter to apply one or more error detecting codes; then the receiver uses the same codes to narrow down exactly where in the message the error (if any) is located. If there is a single bit error in transmission, the decoder can fix the error by

flipping that bit. (Some codes can also address more than one error per message). Other error, correcting method include:

(a) Repetition schemes: If the transmitter repeats each data bit at least three times (triple modular redundancy), the receiver can correct any single-bit error by taking a majority vote of the received data bits.

(b) Parity schemes: If the transmitter sends parity bits covering overlapping groups of data bits, a single –bit error will cause a parity error in every group that includes the erroneous bit. The receiver can correct any single bit error by flipping the one bit that is in every group that fails the check, but not in any group that passes the check. There are a wide variety of party –based codes, differing in exactly how groups of data bit are chosen.

(c) Cyclic redundancy checks: When a transmitter adds a CRC code to a message, a single –bit error will cause the received CRC to differ from the reicever-calcualted CRC. If the message is short enough, the receiver can determine exactly which bit was flipped, and correct it (Header Error Correction).

(d) Hamming distance based checks: Since it takes many bit errors to convert one valid hamming code word to any other valid hamming code word, the receiver can correct any single-bit error in a word by finding the 'closest' valid hamming code, the one code word that has only one bit different from the received word.

Some code can correct a certain number of bit errors and only detect further numbers of bit errors. Codes which can correct one error are termed single error correcting (SEC), and those which detect two are termed double error detecting (DED). Hamming codes can correct single-bit errors and detect double –bit errors (SEC-DED) – more sophisticated codes can correct and detect more errors.

3.9 DATA PROCESSING METHOD

Batch, Online, Real time and Distributed Processing

This is a data processing technique where related transactions are grouped together and transmitted for processing. These transactions are then run or expected to completion without human interaction, so that all input data is pre-selected through scripts or command –line parameters. In batch processing, a program takes a set of data files as input, process the data, and procedures a set of output data files.

On-line processing

Online transaction processing, or OLTP, refers to a transaction processing systems that facilitate and management transaction - oriented applications typically for data entry and retrieval transaction processing. OLTP has also been used to refer to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of such a commercial transaction processing application.

The technology is used in a number of industries, including banking, airlines, mailorder, supermarkets, and manufacturing. Applications include electronic banking, order processing, employee time clock systems, e-commerce, and eTrading.

Real-time processing

Is a transaction processing systems that are subject to a "real-time constraint" – i.e. operational deadlines from even to system response. The needs of real-time software are often addressed in the context of real-time operating systems, and synchronous programming languages, which provide frameworks on which to build real-time application software. A real time system may be one where its application can be

considered (within context) to be mission critical. The anti-lock brakes on a care are simple example of a real-time computing system – the real-time constraint in this system is the short time in which the brakes must be released to prevent the wheel from locking. Real-time computations can be said to have failed if they are not completed before their deadline, where their deadline is relative to an event. A real-time deadline must be met, regardless of system load.

Distributed processing

Distributed processing is the use of more than one processor to perform the processing of an individual task. It also refers to any of a variety of computer systems that use more than one computer, or processor, to run an application. This includes parallel processing, in which a single computer uses more than one CPU to execute programs. More often, however, distributed processing refers to local-area networks (LANs) designed so that a single program can run simultaneously at various sites. Most distributed processing systems contain sophisticated software that detects idle CPUs on the network and parcels out programs to utilize them.

Another form of distributed processing involves distributed databases, database in which the data is stored across two or more computer

systems especially over a network. The database system keeps track of where the data is so that the distributed nature of the database is not apparent to users. A distributed database is a set of database stored on multiple computers that typically appears to applications as a single database. Consequently, an application can simultaneously access and modify the data in several database in a network.

Multi-programming, multi-tasking and multi-processing

Multi-programming

Early computers ran one process at a time. While the process waited for servicing by another device, especially peripheral devices, the CPU was idle. In an input/output intensive process, where large data is been transmitted to and from these input/output devices, the CPU could be idle as much as 80% of the time. Advancements in operating systems led to computers that load several independent processes into memory and switch the CPU from one job to another when the first becomes blocked while waiting for servicing by another device. This is what is being referred to idea to as multiprogramming. It reduces the idle time of the CPU and helps to optimize the CPU capabilities by efficiently using the CPU time.

Programs in a multiprogrammed environment appear to run at the same time. Processes running in a multiprogrammed environment are called concurrent processes. In actually, the CPU processes one instruction at a time, but can execute instructions from any active process.

Multitasking

In computing, multitasking is a method by which multiple tasks, also known as processes, share common processing resources such as a CPU. In the case of a computer with a single CPU, only one task is said to be running at any point in time, meaning that the CPUs is actively executing instructions for that task. Multitasking solves the problem by scheduling which task may be the one running at any given time, and when another waiting task gets a turn. The act of reassigning a CPU from one task to another one is called a context switch. When context switches occur frequently enough the illusion of parallelism is achieved. Even on computers with more than one CPU (called multiprocessor machines), multitasking allows many more task to be run than there are CPUs.

For example, a sales representative could write a letter to prospective clients with a word processing program while simultaneously using a

database program to search for all sales contacts in a particular city of geographic area. Instead of terminating the session with the word processing program, returning to the operating system, and then initiating a session with the database program, multitasking allows the sales representative to display both programs on the computer screen and work with them at the same time.

Operating systems may adopt one of many different scheduling strategies, which generally fall into the following categories:

(a) In multiprogramming systems, the running task keeps running until it performs an operation that requires waiting for an external event (e.g. reading from a tape) or until the computer's scheduler forcibly swaps the running task out of the CPU. Multiprogramming systems are designed to maximize CPU usage.

(b) In time-sharing systems, the running task is required to relinquish the CUP, either voluntarily or by an external events such as a hardware interrupt. Time sharing systems are designed to allow several programs to execute apparently simultaneously.

(c) In real-time systems, some waiting tasks are guaranteed to be given the CPU when an external event occurs. Real time systems

are designed to control mechanical devices such as industrial robots, which require timely processing.

The term time-sharing is no longer commonly used, having been replaced by simply multitasking.

Multi-processing

Multiprocessing is the use of two or more central processing units (CPUs) within a single computer system. The term also refers to the ability of a systems to support more than one processor and/or the ability to allocate tasks between them. There are many various on this basic theme, and the definition of multiprocessing can vary with context, mostly as a function of how CPUs are defined (multiple chips in one package, multiple packages in one system unit, etc).

Multiprocessing sometimes refers to the execution of multiple concurrent software processes in a system as opposed to a single process at any one instant. However, the terms multitasking or multiprogramming are more appropriate to describe this concept, which is implemented mostly in software, whereas multiprocessing is more appropriate to describe the use of multiple CPUs. A system can be both

multiprocessing and multiprogramming, only one of the two, or neither of the two.

SELF ASSESSMENT EXERCISE

- Highlight the common defects in system administration you known.

4.0 CONCLUSION

In this unit, you have learnt about the critical factors for the successful implementation of a management information system, the defect in system administration. You have also learnt about system maintenance, the purpose of system maintenance, corrective maintenance, perfective maintenance and so on.

The unit has also treated succinctly the concept of project management techniques (traditional approach and critical chain) particularly. You have learnt about business systems, the transaction processing and the data processing methods

5.0 SUMMARY

Failure in computerization can usually be traced to the following:

Insoluble technical problems, cost overrun, time overrun, shortfalls in capacity, output deficiency and planning deficiencies.

One of the key reason for failing in management oversight is as a result of organization structure that has not been realized to complement the demands of computerization.

Poor system implementation occurs as a result of inability to interpret and implement user requirements correctly or failure to provide adequate controls.

Project management is the process of planning, organizing and managing resources to bring about the successful completion of specific project goals and objectives. The transaction processing encompasses data entry/capture, data transmission and file updates.

6.0 TUTOR MARKED ASSIGNMENT

* Define and explain the prince 2 process model in project management.

Answers to Self Assessment Exercise

Common defects in system administration are:

a. Inability to control technology and adjust to software updates

b. Inability to react quickly to new developments.

c. Concentration of responsibilities in only few individuals

d. Access to the system by authorized users.

e. Misuse of the system by authorized users.

7.0 REFERENCE/ FURTHER READING

I. K. Oyeyinka & Ayeni (2006): Introduction to Management Information System, Second Edition; Famorks Printers, Lagos.

Olayanju Taiwo (2005): Basic Computer Studies for Schools and Colleges; Daban Printers.

Ojajuni Jethro (2009): Computer and Business Information System; Boomart SCMS Ltd, Lagos, Nigeria.