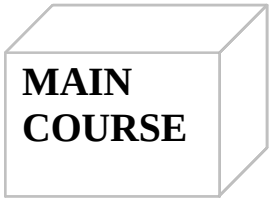
NATIONAL OPEN UNIVERSITY OF NIGERIA

COURSE CODE :MBA 822

COURSE TITLE:
INFORMATION AND TELECOMMUNICATION TECHNOLOGY



MBA 822
INFORMATION AND COMMUNICATIONS TECHNOLOGY

Course Developer/Writer Gerald C. Okereke
Eco Communications Inc.
Ikeja Lagos

Programme Leader Dr. O.J Onwe
National Open University of Nigeria

Course Coordinator Abimbola, E. Adegbola
National Open University of Nigeria

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
5, Dar Es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria.

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Published by
National Open University of Nigeria

Printed 2009

ISBN: 978-058-283-5

Printed by:

CONTENTS PAGE

Introduction

This course, Information and Communications Technology is a compulsory course in the School of Business and Human Resources Management, for those students who wish to obtain a Masters degree in business, finance and related subjects. It is designed to aid business and financial managers in knowing information and communications technologies readily available to enhance speed and accuracy in processing business information.

This course examines the extent to which information and communication has broadened the scope of business and brought about developments in the economy of countries. Country case studies are sited to prove this point, especially in developing economies of the world.

This Course Guide takes you through the nature of the course, the materials you are going to use and explains how you are to use these materials to your maximum benefit. It is expected that at least two hours should be devoted to the study of each course unit. For each unit, there are assessments in the form of tutor-marked assignments. You are advised carry out the exercises immediately after studying the unit.

There will be tutorial lectures to organize for this course. This serves as an avenue to interact with course instructors who will communicate more clearly with you, regarding the course. You are advised to attend the tutorial lectures because they will enhance your understanding of the course. Note that it is also through these tutorial lectures that you will submit your tutor-marked assignment and be assessed accordingly.

Course Aims

This course is designed for you to have an understanding of the critical role that information and communication technology is playing in driving and shaping global economy. It is also for you to acquaint yourself with this technology and see how it is applied to enhance performance in organizations. Discussing the factors that shape the effective applications, abuses and challenges of information communication usage in the society, generally, is also part of the aim of this course.

Course Objectives

Here is a summary of what you should be able to do at the end of this course:

- Identify the positive impact of information and communication technology on the development process
- Identify the information and technology services that enhance development
- Answer the question of trends in ICT investment projects and how beneficial they are
- Define information and communication technology, as well as the information and data
- Identify the qualities and properties of information as it relates to communication technology
- Give reasons for the level and quality of ICT service provision in developing countries
- Explain how to improve the levels of ICT provision
- State the agenda needed to ensure the maximum return to ICT investments in areas such as macroeconomic and education policies
- Identify the benefits associated with information communications technologies like computers etc in the work place
- Identify and differentiate the various types of information communication technology devices
- Explain the benefits of applying networks in business and corporate organizations
- Describe the application of Internet in business through case studies
- Explain the basic architecture of GSM network
- Identify the trends in GSM business in Nigeria
- State the function of a database administrator and the criteria for being one
- Give the various functions of an Operating System as it relates to the working of a information communication technology
- Identify the security and ethical issues associated with information communication technology
- Use a country case study to illustrate the role that information communication technology plays in the economic and development process in any economy, especially in developing economies.

Course Materials

1. The Course Guide

2. Study Units
3. Textbooks
4. The Assignment File
5. Tutorials

Study Units

This course consists of thirteen (13) units, divided into 3 modules. Each module deals with major aspects of the course.

Study Units: The study units of this course are as follows:

Module 1

Unit 1 Basic Concepts of Information and Communication Technology
Unit 2 Information and Communication Technology and Development
Unit 3 ICT and Economic Growth
Unit 4 Introduction to Computers 1
Unit 5 Introduction to Computers 2

Module 2

Unit 1 Computer Communication Networks
Unit 2 The Internet
Unit 3 Global System for Mobile Communications
Unit 4 Database Management System (DBMS)
Unit 5 Operating Systems
Unit 6 Computer System Security
Unit 7 Computer Insecurity

Module 3

Unit 1 Information and Communication Technology and the Society
Unit 2 The Law and Computer Information Systems
Unit 3 Program and Program Languages
Unit 4 Country Case Study: ICT in Alleviating Poverty in India

Ordinarily, you should spend a minimum of 2 hours to study a unit. Start by going through the unit objectives. At the end of the study of the unit, evaluate yourself to find out if you have achieved the objectives of the unit. If not, you would need to go through the unit again.
To help you ascertain how well you have understood the course, there will be exercises mainly in the form of tutor-marked assignments at the

end of each unit. At first attempt, try to answer the questions without necessarily having to go through the unit. However, if you cannot proffer solutions offhand, then go through the unit to answer the questions.

The Assignment File

For each unit, you will find one (1) or two (2) tutor-marked assignments. These assignments serve two purposes:

1. **Self Evaluation: The tutor-marked assignment will assist you to** thoroughly go through each unit, because you are advised to attempt to answer the questions immediately after studying each unit. The questions are designed in such a way that at least one question must prompt a typical self-assessment test.

2. **Obtain Valuable Marks: The tutor-marked assignment is also a** valid means to obtain marks that will form part of your total score in this course. It constitutes 30% of total marks obtainable.

You are advised to go through the units thoroughly for you to be able to proffer correct solution to the tutor-marked assignment.

Assessment

You will be assessed and graded in this course through the tutor-marked assignment and a formal written examination. The allocation of marks is as indicated below:

• Assignments = 30 %
• Examination = 70%

Final Examination and Grading

The final examination will consist of two (2) sections:

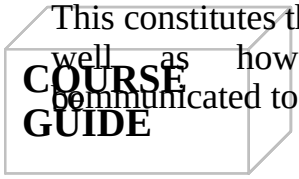
1. Section 1: This is compulsory and weighs 40 marks
2. Section 2: This consists of six (6) questions out of which you are to answer (4) questions. It weighs 60 marks.

The duration of the examination will be 3 hours.

Credit Units

This course attracts 3 credit units only.

The Presentation Schedule



This constitutes the scheduled dates and venue for the tutorial classes, as well as how and when to submit the tutorials. All this will communicated to you in due course.

Course Code MBA 822

Course Title Information and Communications Technology

Course Developer/Writer Gerald C. Okereke
Eco Communications Inc.
Ikeja Lagos

Programme Leader Dr. O.J Onwe
National Open University of Nigeria

Course Coordinator Abimbola, E. Adegbola
National Open University of Nigeria

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Office
5, Dar Es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria.

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Published by
National Open University of Nigeria

Printed 2009

ISBN: 978-058-283-5

CONTENTS **PAGE**

MODULE 1

UNIT 1 BASIC CONCEPTS OF INFORMATION AND COMMUNICATION TECHNOLOGY

CONTENTS

1.0 INTRODUCTION

Information and Communication Technology (IT) is technology that supports activities involving the creation, storage, manipulation and communication of information, together with the related methods, management and application. In other words, IT enables us to record, store, process, retrieve, and transmit information. It encompasses modern technologies such as computers, telecommunications, facsimile and microelectronics. Older technologies such as document filling systems, mechanical accounting machines, printing and cave drawings are also included in the term Information Technology.

Information and Communication Technology in today's world refers to those technologies that determine the efficiency and effectiveness with which we communicate and the devices that allow us to handle information.

Information theory is a branch of mathematics that deals with the measurement of information and its applications in the study of communication, statistics and complexity. It arose out of communication theory as sometimes used to mean the mathematical theory that underlies communication systems. Based on the pioneering work of Claude E. Shannon (1948), information theory establishes the fundamental limits of the communication system and provides guidelines for the construction of practical systems.

Many information scientists accept the standard definition that '**information is data which is used in decision making.' This** definition has a number of implications. One is that is that information is a relative quantity. It is relative to the situation, to the time at which the decision is made and to the decision-makers' background and history. What is of considerable importance in one situation is very possibly totally useless in another. What may be of considerable value to one decision-maker at one time may be likely useless to another decision-maker at a different time or in a different situation. A second implication is that information and decision making are closely intertwined. Information is used only for decision-making and decision makers have only the resources of information available to them.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- define information and communication technology, as well as the information and data
- identify the qualities and properties of information as it relates to communication technology
- answer the question of what is the value of information
- explain the steps that are taken in processing data into information.

3.0 MAIN CONTENT

3.1 Properties of Information

There are properties associated with information that determine the usefulness of information. The three main factors or characteristics related to information usefulness are:

Information Quality: how good the information is, based on precision, completeness, timeliness, and source.

Information Accessibility: how easy it is to obtain and manipulate the information, regardless of how good it is.

Information Presentation: the level of summarization and format for presentation to the user, regardless of how good the information is and how accessible it is.

Because preventing inappropriate or unauthorized use of information is also crucial, a fourth area of characterizing and evaluating information is **information security, the extent to which information is controlled and** protected from inappropriate, unauthorized, or illegal access and use.

Each of the four factors is subdivided into more detailed characteristics of information as stated below:

Accuracy: This is the extent to which information represents what is supposed to be represented. Increasing accuracy is an important purpose of information system.

Precision: This related term iìtracking an advertising campaign are generally satisfied with week-old data. For other tasks such as long-term planning, data from months or even years before may be satisfactory because some long-term trends change slowly and predictably.

Age: This is the amount of time that has passed before the data was produced. The age of data produced daily, weekly or monthly by a firm's information system is easy to determine. The age of data from other sources may be less apparent. For example population data used in creating the sample for a marketing survey might be based on the last census or on more recent data such as population changes since the census.

Source: The source of data is the person or organization that produced the data. The source is often the tip-off the bias; for example when one economic forecaster tends to be more optimistic than another. Data sources may be internal or external to the firm. Combining and reconciling data from internal and external sources is crucial in analyzing the business environment.

Availability: This is the extent to which the necessary information exists in an information system and can be accessed effectively by people who need it. For example, information on a corporate mainframe computer may not be available in a timely version if a potential user cannot download it to his personal computer. Similarly, even what can be derived from paper documents in a file cabinet in the user's own office may be unavailable if the analysis process will take too long because the information is on paper.

Admissibility: The admissibility of information depends on whether laws, regulations or culture require or prohibit its use. This is an important factor when age, gender, marital status, ethnicity, or medical condition might be viewed as relevant by some people and inappropriate by others. Such situations occur frequently in the course of business decision making such as hiring and promotion, assigning work tasks, determining insurance rate and making loans.

Level of Summarization: This is the comparison between the number of items in the original data and the number of data displayed. For example, a report combining 600 products into 4 product groups is more summarized (and less detailed) than a report combining the 600 products into 23 product groups.

Format: This is the form in which information is organized and expressed or displayed to the user. Format involves things ranging from the number of decimal places displayed in numbers through the different ways to present the same material graphically.

3.2 The Qualities of Good Information

The general characteristics of information should suggest the qualities of good information. The basic qualities of good information are:

1. **Relevance: Information must be relevant to the purpose for which** the manager wants to use it. In practice too many reports fail to 'keep to the point' and contain purposeless, irritating paragraphs which only serve to vex the manager's reading time.

2. **Completeness: An information user should have all the information** he needs to do his job properly. If he does not have a complete picture of the situation, he might make bad decisions.

3. **Accuracy: Information should be accurate because using incorrect** information could have serious and damaging consequences. However, information should only be accurate enough for its purposes and there is no need to go into unnecessary details for pointless accuracy.

4. **Clarity: Information must be clear to the user. If the user does not** understand it properly, he cannot use it properly. Lack of clarity is one of the causes of breakdown in communication which is referred to in information system theory as 'noise'. Noise is therefore caused by incompleteness, irrelevance, excessive volumes of information and lack of clarity.

5. Confidence in the Information Received: Information should be accurate and the person to whom it is communicated should also be confident that it is accurate. The quality of communication is determined by the confidence that key people throughout an organization have in each other's ability. Communication between managers or between managers and employees can help to increase their confidence and thereby improve performance. A manager who is impressed by someone he meets and talks to will put his confidence in that person, and work with him more readily. Simple greeting at first meeting is a means of promoting confidence.

6. Communication to the right person: Within an organization, individuals are given the authority to do certain tasks, and they must be given the information they need to do them.

7. Volume of information: There are physical and mental limitations to what a person can read, absorb and understand properly before taking action. An enormous mountain of information, even if it is relevant cannot be handled. Reports to management must therefore be clear and concise.

8. Timing of Information: Information which is not available until after a decision is made will be useful only for comparisons and longer term control, and may serve no purpose even then. The time value of information may be gauged by the latest event (time) which the information covers; and the comparison and control action for which it will be used. Delays in communicating information might make the information useless or it might delay any decisions or action by the information user.

3.3 The Value of Information

Information should have some value; otherwise it would not be worth the cost of collecting and filing it. The benefits obtainable from the information must also exceed the costs of acquiring it, and whenever management is trying to decide whether or not to produce information for a particular purpose (e.g. whether to computerize an operation or to build a planning model) a cost/benefit study ought to be made.

For information to have value, it must lead to a decision to take action which results in reducing costs, eliminating losses, increasing sales, better utilization of resources, prevention of fraud (audit requirements) or providing management with information about the consequences of alternative courses of action.

Information that is provided but not used has no actual value. A decision taken on the basis of information received also has no value. It is only the action taken as a result of a decision that realizes actual value for a company.

As the value of information lies in the action taken as a result of it, an assessment of value may be reached by asking the following questions:

1. What information is provided?
2. What is it used for?
3. Who uses it?
4. How often is it used?
5. Does the frequency with which it is used coincide with the frequency with which it is provided?
6. What is achieved by using it?
7. What other relevant information is available which could be used instead?

An assessment of the value of information can be derived in this way, and the cost of obtaining it should then be compared against this value. On the basis of this comparison, it can be decided whether certain items of information are worth having.

Deciding whether it is worthwhile to have more information should depend on the marginal benefits expected from getting it and the extra costs of obtaining it. The benefits of more information should be measured in terms of the difference it would make to management decisions if the information were made available. Most information is only worthwhile if it might make the user/decision-maker change his or her mind from what it would otherwise have been if the extra information had not been there.

Since the increment cost of obtaining extra qualities of information will eventually exceed the marginal benefits derived from them, there will inevitably be a limit to the economic size of a management.

The greater the accuracy of information provided, the more it will cost. At the high levels of accuracy, it is probable that the marginal costs of extra accuracy will exceed its marginal benefit value. It is most likely; therefore, that management will be satisfied with imperfect information and would not expect perfection.

The value of information must also relate to the frequency of its provision, and to the level in the management hierarchy where it is sent and used.

3.4 Sources of Information

Information comes from sources both inside and outside an organization, and an informative system should be designed so as to obtain all the relevant information from the necessary sources:

1. Gathering data/information from inside the organization involves:

- Establishing a system for collecting or measuring data-e.g. measuring output, sales costs, cash receipts and payments, assets purchases, stock turnover etc. In other words, there must be established procedures for what data is collected (how frequently, by whom, by what methods etc) and how it is processed, filled and communicated.

- Relying to some extent on informal communication of information between managers and staff (e.g. by word-of-mouth, at meetings etc).

2. Entrusting particular individuals to obtain information from outside the organization.

Formal collection of data from outside sources includes the following:

- A company's tax specialists will be expected to gather information about changes in tax laws and how this will affect the company.
- Obtaining information about any new legislation on health and safety at work, or employment regulations, must be the responsibility of a particular person.
- Research and development work often depends on information about other research work and development work being done by other companies. An R&D official might be made responsible for finding out what he can about what R&D is going on outside the company.
- Marketing managers need to know about the opinion and buying attitudes of potential customers. To obtain this information, they might carry out market research exercises.

Informal gathering of information from outside sources often goes on all the time, consciously or unconsciously, because the employees of an organization learn from newspapers and television reports what is going on in the world around them.

Some characteristics such as accuracy can be measured without regard to the way information is used. Others such as timeliness and completeness depend on how the information is used and sometimes on the user’s personal work style.

3.5 Information Processing

The goal of information/data processing is to produce meaningful information. The processing of data and the delivery of information have been the basic requirements of people and organizations since the dawning of civilization. Individual organizations and whole societies depend on information for their well being and for their very survival.

Computers are useful devices for processing data and helping to assign meaning to them. These activities can be completed quickly and accurately through the use of computers. However, information processing is fundamentally a human activity. People are information processors. People use processing techniques to help them cope with myriad of details involved in day-to-day living.

Information processing consists of a set of procedures that transform data and information. Basically the procedures include data collection, recording, sorting, classification, calculation, storing, retrieving.

1. Data Collection: Data collection is the act of seeking information or additional information about a problem or needs under investigation. During this process, emphasis is given to the strengths and weaknesses of the existing data.

Data collection requires that two steps be performed in sequence. The first step is to identify and locate the various sources of data. The second is to actually collect the data.

Generally, to identify and locate various sources of data, there are both internal sources and external sources. The major internal sources among others are organizational charts; forms and documents; procedure manuals; financial reports; data processing and documentation manuals; top, middle and low level managers; other employees of the organization; etc. Some of the external sources include computer manufacturers and vendors; customers; suppliers; stockholders; government documents; local, state and federal government agencies; competitors; newspapers; journals, textbooks, external consultants and other professional groups.

The second step, which is to actually collect the data, requires a number of tools such as interviews, direct observation, and the development of questionnaires. In a structured interview, the questions are written in advance, but in an unstructured interview the questions are not written in advance. Other collection techniques employed are telephone calls and simulation.

2. Recording: To record or capture data means that facts are brought into a processing system in useable form.When they are recorded, data become available for processing. Within a business organization, data are often recorded in handwritten or typewritten form on source documents that contain data representing business transactions. Source documents provide records of the transactions. As the term implies source documents are the sources of data to be processed.

When you visit a bank to deposit or withdraw money, the transaction data are recorded on your deposit slip or check. The data from these documents trigger a series of processing activities to update your financial status with the bank.

3. Sorting: One of the simplest ways in which people assign meaning to data is through sorting. To sort means to arrange data in predefined sequence. Data can be sorted alphabetically or numerically in either ascending or descending sequence. Sorting might be performed as a preliminary step before applying one of the other processing techniques. Or, the actual sorting itself may transform data into information.

Consider the example of a telephone directory. Just the simple act of arranging the names of the people in alphabetic order gives meaning to the listings. Without this sorting, the directory would be practically worthless.

Business information processing uses sorting techniques extensively. Virtually all records within business files are maintained in some logical sequence. File folders, for example, are indexed according to people's names, subject areas or identification numbers. The folders are arranged within a filing cabinet to make it easy to locate and retrieve files.

4. Classifying: Data can be assigned meaning by classifying them. To classify means to categorize - to place data with similar characteristics within the same category, or group. Information concerning the group itself then can be projected to the items that were placed in the group.

Classification is one of the main ways be which people deal with the complexities of everyday life. New data or experiences are classified into kinds of familiar categories such as friends, automobiles, food, school, subjects, clients etc, to provide bases for understanding and using the data.

Classification is a common method of processing business data. For example, accounting systems are primary systems. Amounts of money representing income and expenses are categorized by source and used by managers to gain an understanding of the ongoing status of the company. Financial data are classified into assets, liabilities, and ownership interest to present an overall picture of the organization. Without such a classification method, business managers would be overwhelmed with financial data but would lack meaningful information.

5. Calculating: To calculate data means to apply arithmetic operations to data. These functions include addition, subtraction, multiplication, division or other higher-level mathematical functions. When calculations are applied to data, new values represent additional information.

The business world uses calculation extensively. For example, consider what happens when you purchase items from a retail store. The sales clerk uses arithmetic to provide you with information on the amounts owed for the purchase of merchandise. The number of items purchased is multiplied by the price of each item. All of these amounts are totaled, the sales tax is calculated and the amount of change you are due is computed. The figures derived through calculations represent information required to complete a sale.

6. Summarizing: Sometimes, a person is faced with too much data. All of the facts and figures result in information overload with the essential information hidden among unwanted details. In such a case, summarizing techniques are applied. To summarize is to condense or to reduce a large mass of details to a more manageable size and to extract the essentials. Business managers operate on the basis of summary information. Managers would be overwhelmed if they tried to cope with all of the facts and figures that represent the hundreds or thousands of business transactions that occur in a large business each day. Little time would be left for managing.

7. Comparison: In many instance data only take a meaning when they can be compared with other data. A fact or figure in isolation may be meaningless. But when that item of data is placed next to other data that already have information content, useful knowledge can result. To compare is to evaluate a data item against some known facts or quantity. This comparison provides meaning. A large part of a business manager's job is to make comparisons and to act on the findings.

3.6 The Information Processing Cycle

The four basic information processing activities – input, processing, output, and storage – typically are performed in logical sequence. Data originate as source documents and are prepared for input. After being input, the data undergo the actual processing steps. The resulting information then is communicated to users or retained for later processing and output.

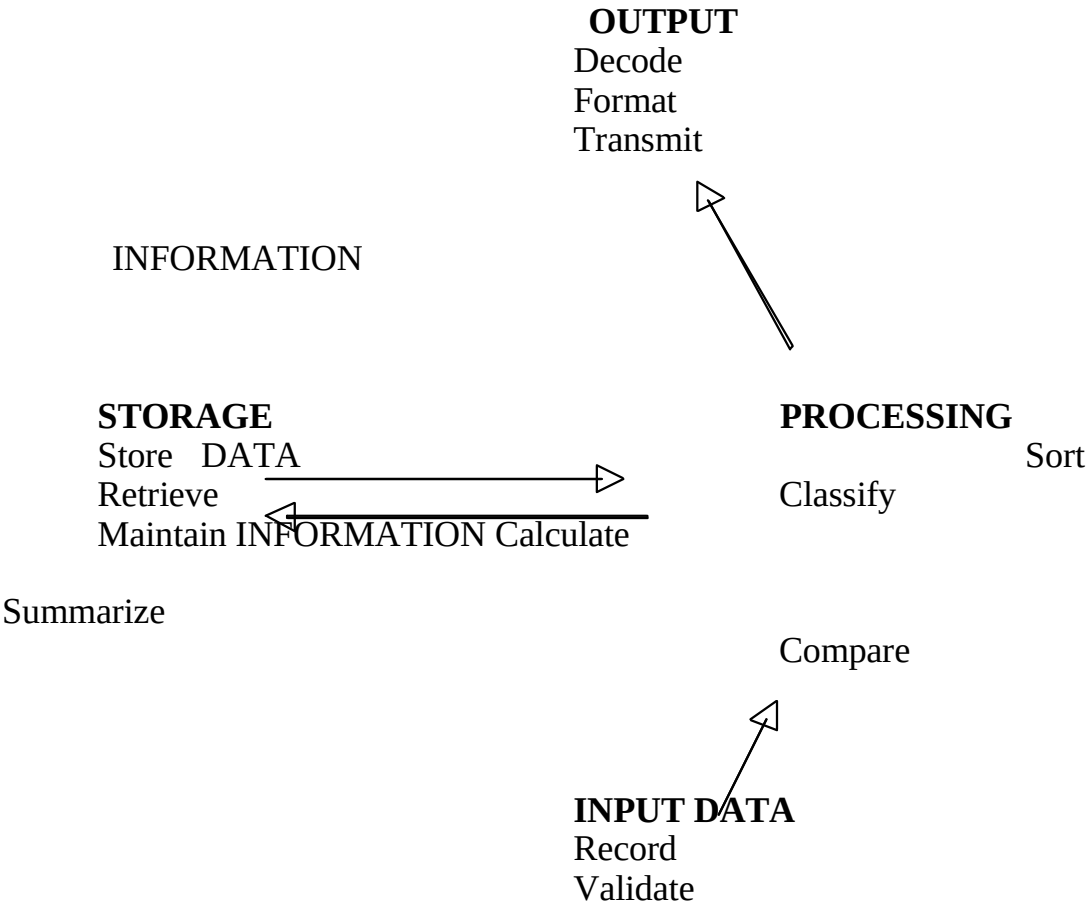


Figure 1: The information processing cycle

4.0 CONCLUSION

Truly we are in the information age in which all human activities are driven by the efficiency in the utilization of information. All the advances in technologies are geared towards making information readily available. Prior to the entrance of modern day technologies, man for the conversion of raw data into useable information had developed standard formats. All advances in the processing of information build upon the building blocks. Therefore, a thorough understanding of the concept of information goes a long way in making you appreciate information and communication technology.

5.0 SUMMARY

This unit has highlighted the following points:

- Many information scientists accept the standard definition that "information is data, which is used in decision making." This definition has a number of implications. One is that is that information is a relative quantity.

- Information theory is a branch of mathematics that deals with the measurement of information and their applications in the study of communication, statistics and complexity.

- There are major properties associated with information that determine the usefulness of information. These are quality, accessibility and presentation.

- Information must be relevant to the purpose for which the manager wants to use it. In practice too many reports fail to 'keep to the point' and contain purposeless, irritating paragraphs which only serve to vex the manager's reading time.

- Information should have some value; otherwise it would not be worth the cost of collecting and filing it. The benefits from the information must also exceed the costs of acquiring it.

- Deciding whether it is worthwhile having more information should depend on the marginal benefits expected from getting it and the extra costs of obtaining it.

- Information comes from sources both inside and outside an organization, and an informative system should be designed so as to obtain all the relevant information from the necessary sources.

- Informal gathering of information from outside sources often goes on all the time, consciously or unconsciously, because the employees of an organization learn from newspapers and television reports what is going on in the world around them.

- The goal of information/data processing is to produce meaningful information. The processing of data and the delivery of information have been the basic requirements of people and organizations since the dawning of civilization.

7.0 REFERENCES/FURTHER READINGS

Anderson, R.G (1994). Data Processing: Principles & Practice, Vol. 1. Pitman Publishing.

Anderson, R.G (1994). Data Processing: Information Systems & *Technology, Vol. 2. Pitman Publishing.*

French, C.S. (1993). Computer Studies. DP Publishing Ltd.

Norton, P (1995). Introduction to Computers. McGraw-Hill: Macmillan.

UNIT 2 INFORMATION AND COMMUNICATION TECHNOLOGY AND DEVELOPMENT

CONTENTS

1.0 INTRODUCTION

Information and communication technology (ICT) has a critical role to play in development efforts round the world. There was a time when ICT's role in fighting poverty and promoting economic growth were not widely understood. Many in the development community questioned how high-tech (and often expensive) communications technology could be used to alleviate such dire challenges as starvation, homelessness and lack of basic education and health services. Lately however, this view has given way to an understanding of ICT as an essential component of border efforts to harness the free flow of information to increase voice, accountability and economic development.

In recent years, developing countries and the international development community have started taking concrete actions to incorporate ICT into their economic policies and development agenda. Many countries are implementing national e-strategies that emphasize the ubiquity of connectivity as well as new applications in areas such as e-government and e-business. The Millennium Development Goals (MDGs), drawn from the United Nations Millennium Declaration and adopted in September 2000 have several specific targets involving ICT as a tool for reducing poverty. Nevertheless, improving the identification and measurement of the actual benefits of applying ICT remains an important challenge, especially in the light of the rapid change in the sector and the dearth of concrete and long-term data across countries.

In recent years the world's policy makers have recognized that ICT provides key inputs for economic development, contributes to global integration, and enhances public sector effectiveness, efficiency, and transparency. There is also a growing consensus that countries seeking to strengthen their investment climates (for foreign as well as domestic investors) should make it a priority to improve ICT access and quality. Country conditions that bolster ICT investment include sound economic policies, strong property rights, liberalized markets, and limited

restrictions. Recent progress and lessons on entry and ownership, and predictable regulation contribute to a healthy overall business environment and so to growth throughout the economy. Firms that use ICT grow faster, invest more, and are more productive and more profitable than those that do not. For example, sales growth is 3.4 percentage points higher and value added per employee $3,400 more among developing country firms that use e-mail to communicate with clients and suppliers. Profits are substantially higher among firms using ICT.

The international community is increasingly committed to the monitoring and evaluation (M&E) of development programmes. The World Bank Group has sharpened its focus on results in its own strategies, operations, diagnostic work and instruments. It has put a premium on better measurement of outputs and outcomes in order to assess progress toward well-defined goals, increase accountability, and better understand the Bank's contribution to sector performance--ultimately supporting policy advice and decision making.

In response to the call for increased M&E efforts for ICT by the development community, most notably during the World Summits on the Information Society held in Geneva in 2003 and Tunis in 2005, The Global Information and Communication Technologies Department (GICT) is undertaking several initiatives to advance methods of monitoring results in ICT for development projects.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- identify the positive impacts of information and communication technology to the development process
- identify the information and technology services that enhances development
- answer the question of trends in ICT investment projects and how beneficial they are
- trace the trend in mobile ICT projects in Nigeria.

3.0 MAIN CONTENT

3.1 The Role of ICT in Development

In the past few decades, information and communication technology (ICT) has transformed the world. Its potential for reducing poverty and

fostering growth in developing countries has increased rapidly. Mobile telephones provide market links for farmers and entrepreneurs. The Internet delivers vital knowledge to schools and hospitals. Computer improves public and private services and increases productivity and participation. By connecting people and places ICT has played a vital role in national, regional and global development and holds enormous promise for the future.

It has been over 20 years since the first telephone company was privatized, 10 since the World Wide Web emerged, and 5 since the telecommunications bubble burst. How has ICT driven and evolved in response to these and other events? What has been learned about ICT trends and the policies that shape an information society? And how can further advances be fostered and facilitated?

When tailored to needs, ICT has the potential to raise growth in **businesses of any size and countries at any stage of development.** Related but even more important, is ICT's role in reducing poverty and inequality, both within and across countries. Thus it is crucial that ICT move closer to the mainstream of development economics and policies--nationally, regionally, and globally. Given ICT's far-reaching payoffs--and the many efforts required to achieve them-- this report is aimed not only at ICT experts but also at the broader development community.

ICT plays a vital role in advancing economic growth and reducing poverty. Research in the 1960s and 1970s showed how telecommunications strengthens economic production and distribution, public service delivery, and government administration. In the 1980s information became recognized as a crucial factor of production, along with capital and labour; in the 1990s globalization and the increasing information intensity of economic activity, coupled with rapid technological change and increase in their competitiveness have promoted growth and expanded opportunities for poor people in developing countries. ICT is an essential part of national infrastructure and private sector potential. It can create business opportunities, especially for companies located far from urban centers, and improve links among firms, suppliers, and clients. When used well, ICT can also **make management and operations more efficient. The Internet can be** especially valuable for firms in developing countries because it provides opportunities to connect to markets and participate in trade, domestic and foreign. A recent survey of 56 developed and developing countries found a significant link between Internet access and trade growth--with the greatest benefits accruing to developing countries with the weakest trade links.

As with other factors of production, such as capital and labor, ICT use differs based on business size, ownership, and export orientation. In developing countries Web site and computer (though not necessarily e-mail) use are more common among service firms than firms engaged in manufacturing, agro industry, and construction. Web site and e-mail use are especially high in the telecommunications, information technology, real estate, and hotel and restaurant industries, and among exporters and foreign-owned firms. Among regions, firms in Central and Eastern Europe use such technology the most, reflecting its correlation with national income. But Web sites and e-mail are also widely used in some low-income countries--Bangladesh, Kenya, Moldova, and Tanzania--suggesting that ICT is not a luxury.

ICT is also crucial to sustainable poverty reduction, because it makes a country's economy more efficient and globally competitive, improves health and education services, and creates new sources of income and employment for poor people. In addition, ICT enhances social inclusion and promotes more effective, accountable, democratic government, especially when combined with effective freedom of information and expression.

3.2 ICT Services and Development

Over the past 25 years, developing countries have considerably increased ICT access, especially for telephone services. Developing countries account for more than 60 per cent of people.

Mobile Phones

Most of the recent growth has involved mobile phones which now outnumber fixed ones. In Nigeria the number of mobile phone subscribers jumped from 370,000 in 2001 to 16.8 million in September 2005, making the mobile phone market the second largest in Africa. In the Philippines, which has had more mobile than fixed telephone subscribers since 2000, mobile phone subscribers continue to multiply. By the end of 2005, the country had about 40 million mobile subscribers--six times more than in 2000.

Mobile phones have an especially dramatic impact in developing countries--substituting for scarce fixed connections, increasing mobility, reducing transaction costs, broadening trade networks, and facilitating searches for employment. With prepaid services and calling cards, even poor households have been able to benefit from increased telephone access.

Telephone services now reach many small cities and towns, and by 2005 half of the world's households had telephones. Among developing regions the telephone subscription rate is highest in Europe and Central Asia, subscription rate is highest in Europe and Central Asia, per 1,000 people. But growth was highest in Sub- Saharan Africa, with the rate tripling--albeit to a still-low 103 subscribers per 1,000 people.

The Internet

Other types of ICT have also expanded rapidly in recent years. The latest estimates indicate that worldwide, Internet use more than quadrupled between 2000 and 2005. Again Europe and Central Asia is in the lead among developing regions, with 117 Internet users per 1,000 people in 2004- four times as many as in 2000 and six to eight times as many as in South Asia and Sub-Saharan Africa. During this period services remain closed or barely open in about half of developing countries. Effective competition between multiple providers helps expand access and results in cheaper, more modern services. In 2003, 130 of 164 countries with available data had at least three competing providers of mobile services. The Democratic Republic of Congo has six competing mobile telephone operators, giving it a mobile density 13 times that of Ethiopia--which has a similar income per capita but just one operator. In Algeria almost no one had a mobile subscription in 2000. But in 2003, after a second operator began providing services, nearly 5 per cent of people did--and when a third operator entered the market in 2004, that share leapt to more than 15 per cent by the end of the year and to 32 per cent by September 2005. Similarly, Grenada issued new licenses in 2002, and between 2000 and 2004 the number of mobile subscribers soared from 45 to 860 per 1,000 people.

In markets for international telephone services, full competition leads to prices about half those in countries with limited competition. Among 30 African and Latin American countries that undertook telecommunications reforms in the 1980s and 1990s, those that introduced competition saw the sector grow and costs fall faster than those that delayed competition.

The Internet has also spurred a growing wave of innovation, ushering in new services and more cost-effective network solutions--especially in countries where service providers are allowed to build their own networks and gateways. New wireless technology is resulting in innovative business models and holds the promise of connecting poor users, extending competition to all market segments, and accelerating development of broadband infrastructure and access. Such technology is affordably priced and commercially viable in a number of countries, in

both urban and rural areas. For example, a single broadband Internet connection in a village can provide access for numerous corporations from institutional programmes (such as e-government and computers in schools) and private users.

3.3 Investments in ICT Development Projects

Privatization and technological advances have boosted foreign direct investment (FDI)--a major source of ICT financing. In 1988 Chile privatized its incumbent operator, triggering the first wave of telecommunications-related FDI in developing countries, typically through divestitures of state companies to foreign investors. Since then more than 80 developing countries have privatized their incumbent telecommunications providers.

A second wave of telecommunications FDI started in the mid-1990s as governments, aiming to increase access to and revenue from communication services, awarded new licenses for mobile telephony and encouraged foreign investment. In 2003 mobile projects accounted for 51 per cent Africa, creating a bigger role for financial and regional investors. The region's three largest mobile phone operators accounting for nearly half of telecommunications FDI are all regional firms.

But growing South-South investment is also due to growing wealth and capital account liberalization in some emerging market economies--trends that have increased the supply of capital in these countries and enabled their companies to invest abroad. By 2002, 4 of the 30 largest international telecommunications corporations were from developing countries. Other factors favoring South-South investment include geographic proximity and ethnic and cultural ties. Most South-South telecommunications investors stick to their home or neighboring regions: during 1990/2003 more than 85 per cent of such FDI stayed in the same region. Countries that avoid imposing unnecessary requirements that might exclude otherwise qualified bidders, and create a level playing field that provides fair opportunities to new entrants regardless of size or origin, are more likely to attract South- South and regional FDI.

Consistent, predictable, and transparent sector policies and regulation are essential to remove market impediments. Obstacles to well-functioning markets often remain even after extensive sector reforms. In Peru all segments of the telecommunications market have been open since 1995, but telephone services in provincial towns and marginal areas of big cities remain well below the levels achieved in other developing countries with comparably open markets. The challenge everywhere is to enable operators to tailor their

service offerings and technical choices as effectively and efficiently as possible.

During both waves of telecommunications, foreign investors were seeking new markets, higher returns, and diversified exposure. Many governments welcomed FDI as a way to expand networks, develop new services, and generate revenue through license fees. FDI also brought stronger, longer commitments than did other types of foreign investment, as well as new skills, technology, and management approaches. Between 1990 and 2003, 122 of 154 developing countries received foreign investment in telecommunications.

FDI in telecommunications jumped from $2 billion in 1990 to $33 billion in 1998--but gradually fell to about $13 billion in 2002 and 2003. Still, the decline in FDI has been smaller for telecommunications than for other infrastructure sectors. And although FDI to acquire government assets dropped significantly after 2000, flows for sector expansion stayed at the same level as during the boom years.

During 19902003, telecommunications projects accounted for 12 percent of FDI in developing countries. Latin America and the Caribbean attracted more than half of FDI in telecommunications, while Europe and Central Asia received about a quarter. These large shares reflect the prominence of middle-income countries in telecommunications FDI: during 1990-2003 low-income countries received just 6 percent of such investment.

Developing countries are home to a growing number of FDI providers. Although the largest foreign direct investors in telecommunications are multinational Europe and the United States, in recent years FDI originating in developing countries has become a fast-growing trend. By 2003 these South-South investments accounted for more than a quarter of telecommunications FDI in developing countries, up from a negligible share in the early 1990s. Most such investment came from countries that were among the early liberalizes in their regions. Some investors from developed countries have reduced FDI due to the bursting of the telecommunications bubble in 2000, compromised balance sheets following major investments or acquisitions, disappointing returns on some projects (both at home and abroad), and pessimism about emerging markets. For example, many global players invested in the developing markets of Latin America and East Asia during the 1990s, but have since withdrawn. Global operators have also pulled out of Sub-Sahara.

3.4 Mobile FDI in Nigeria

Following the adoption of the National Telecommunications Policy in 2000 and the award of three GSM (Global System for Mobile Communications) licenses to private operators in 2001, mobile investment and network rollout increased rapidly in Nigeria. The most dynamic new entrant was Mobile Telephone Networks (MTN) of South Africa, which achieved a 42 per cent market share by March 2005. Globacom followed (100 percent held by local shareholders) with a 24 percent market share, V-Mobile (majority-owned by private investors) with 24 per cent, and then M-Tel (fully owned by state-owned incumbent NITEL) with 10per cent. New mobile subscriptions increased from about 28,250 per month during 2001 to more than 500,000 per month in 2004, raising the number of mobile subscribers from 370,000 in 2001 to about 11 million by March 2005. Mobile penetration rates rose from 0.3 percent to 8.2 percent over the same period. Industry reports estimate that foreign investment in the telecommunications sector had reached $3.5 billion by the end of 2004, making it the second biggest recipient of private investment in the country, behind only the oil and gas sector. Mobile telephony represented more than 70 per cent of this investment, at $2.5 billion.

3.5 Factors for ICT Development

Capital is crucial to the development and expansion of robust telecommunications networks. Because developing countries often lack the capital--as well as the technology and managerial know-how--needed to develop such networks, many have turned to private investors, domestic and foreign. By opening their telecommunications markets through well-designed reforms, governments can create competitive markets that grow faster, lower costs, facilitate innovation, and respond better to user needs. As a result, the traditional monopoly model of telecommunications services—based on extensive state control and protected national markets--has eroded, in concert with rapid technological advances in the sector and fundamental changes in economic policy in developing countries. Over the past two decades telecommunications markets have undergone unprecedented liberalization in every region--though the pace and scale of reform have varied, and markets for fixed local and international telephone.

Liberalization and competition--and the resulting increase in private investment--have driven the development of, telecommunications infrastructure and ICT in general.

The regulatory improvements needed to achieve that goal often include opening markets to new entrants (including small domestic entrepreneurs), rebalancing retail tariffs, establishing an effective cost-based interconnection regime, securing reasonable access to existing infrastructure, and making radio spectrum available to a wider range of

service providers. Consistent and transparent processes--for legal, regulatory, and administrative procedures and institutions--are the main requirements. Some traditional regulatory provisions may stand in the way of new technologies, decentralized supply, and other innovations. In addition, high taxation can discourage investment by telecommunications operators and suppress demand; and as the cost of manufacturing cell phones continues to fall, government taxes and duties on their import, sale, and use remain a binding constraint on extending information and communication services to poor people.

4.0 CONCLUSION

Information and Communication Technology has played obvious roles in global development process by making the world a potential and continual emerging global village for business and social interactions. The challenge of the dynamic nature of ICT which sometimes makes it difficult to have more accurate data on its impact on global development, remains to be contended with. However, even if tracking the process with data is challenging, the obvious positive impact of ICT on development process, even in developing economies cannot be denied.

5.0 SUMMARY

The following are salient issues arising from discussing the role of ICT in development:

- Information and communication technology (ICT) has a critical role to play in development effort round the world.

- In recent years the world's policy makers have recognized that ICT provides key inputs for economic development, contributes to global integration, and enhances public sector effectiveness, efficiency, and transparency.

- In the past few decades, information and communication technology (ICT) has transformed the world. Its potential for reducing poverty and fostering growth in developing countries has increased rapidly.

- When tailored to needs, ICT has the potential to raise growth in **businesses of any size and countries at any stage of development.**
- ICT is also crucial to sustainable poverty reduction, because it makes a country's economy more efficient and globally competitive.

- Mobile phones have an especially dramatic impact in developing countries--substituting for scarce fixed connections, increasing

mobility, reducing transaction costs, broadening trade networks, and facilitating searches for employment.

- The Internet has also spurred a growing wave of innovation, ushering in new services and more cost-effective network solutions--especially in countries where service providers are allowed to build their own networks and gateways.

- Privatization and technological advances have boosted foreign direct investment (FDI)--a major source of ICT financing.

- Developing countries are home to a growing number of FDI providers.

- During 19902003, telecommunications projects accounted for 12 per cent of FDI in developing countries.

- Capital is crucial to the development and expansion of robust telecommunications networks. Because developing countries often lack the capital--as well as the technology and managerial know-how--needed to develop such networks, many have turned to private investors, domestic and foreign.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss the ICT services that have enhanced developments in the economy and society.
2. Enumerate at least 5 ways in which ICT has helped in the development processes.

7.0 REFERENCES/FURTHER READINGS

Odukoya, Atinuke (2005). "Engendering the Information Society in Nigeria". Women Magazine. DevNet Publication.

Zhen-Wei Qiagn, Christien et al(2004). "Contribution of ICT to Economic Growth". World Bank Working Paper, No 24.

Zhen-Wei Jiegn, Christien et al (2004). "Factors Influencing the Contribution of ICT to Economic Growth". World Bank Working *Paper, No 24.*

Jerry Grace, et al. "ICT and Broad Based Development". World Bank *Working Paper, No 12.*

Zhen-Wei Qiang et al (2006). “Information and Communication for Development: Trends and Policies”. World Bank Paper Vol. 1:1.

UNIT 3 ICT AND ECONOMIC GROWTH

CONTENTS

1.0 INTRODUCTION

Information and communication technologies (ICTs) are the tools that facilitate the production, transmission, and processing of information. Thus a broad base definition of ICTs range from traditional technologies such as the printed word, to the most modern communications and data delivery systems such as terrestrial satellites that can download digital data to a laptop hooked up to a cellular network. Such a broad definition risks missing trees for the forest, however.

Perhaps the simplest way of demonstrating the importance of ICTs in the development process is to examine the willingness of the poor to pay for service. As Figure 2 shows, the poorest quintile of the population in Chile considers telecommunication such a basic service that they spend more of their income on telecommunication than on water. Further more an average Chilean spends more of his income on telecommunication than on electricity and water combined. This disproportionate expenditure is a reflection of the perceived opportunities associated with acquiring ICTs. The capacity to raise income and to improve the economic growth rate alone is an enticing incentive, but ICTs also offer opportunities to improve the environment, educational outcomes, and health service delivery, as well as other government services.

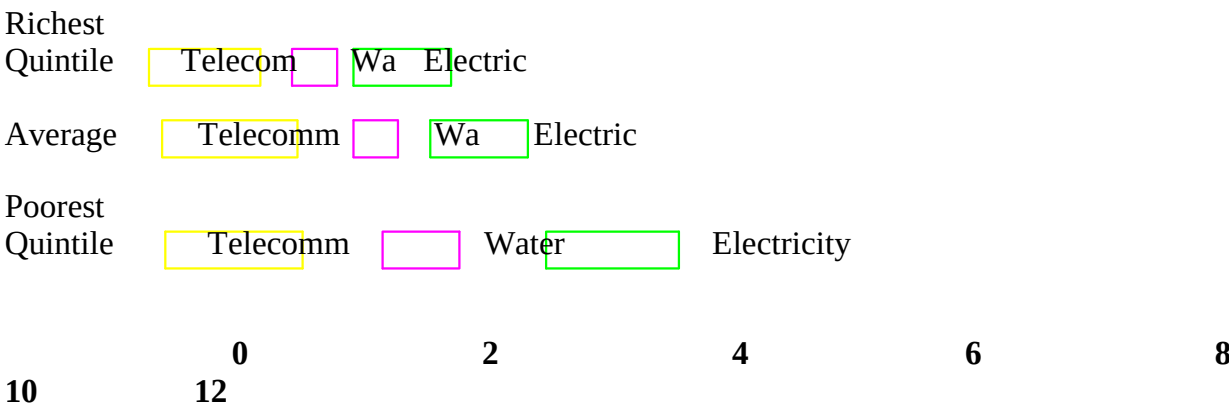
2.0 OBJECTIVES

At the end of this unit you should be able to:

- explain the role of ICT in development
- state the reasons for the level and quality of ICT service provision in developing countries
- explain what to do to improve the levels of ICT provision
- identify the agenda needed to ensure the maximum return on ICT investments in areas such as macroeconomic and education policies
- explain how ICT brings about accumulating capitals in an economy.

Percentage of Income

Fiure 2: Percentage of expenditure on utilities in Chile by income (Poorest and richest quintile and averages)



3.0 MAIN CONTENT

3.1 How ICT Helps the Development Process

The variety of technologies incorporated under the term ICT operate differently and have unique effects based on the manner in which they are used. Nevertheless, their relationship to economic and social development all stem from several basic characteristics related to improved information production and sharing. These include the following:

1. Sharing Knowledge: The single most important benefit associated with access to new ICTs such as telecommunications and the Internet is the increase in the supply of information. Reducing the cost of producing and transmitting information increases its availability and accessibility, which in turn reduces uncertainty. Reduced uncertainty will generally lead to better decision making and allow for new forms of organizational innovation, thus reducing transaction costs and inefficiencies. The fundamental idea behind the 'digital' or 'new' economy is that value added is increasingly concentrated in the application of new ideas to existing systems. Consequently, productive capacity no longer relies solely on investments in plants and labour, but in adapting new technologies and organizational forms into existing forms of economic activity.

2. Increasing Productivity: The use of ICTs benefits productivity through the creation of models for turning inputs into products

and/or services. As organizations learn and adapt to new technologies, labour can be redeployed to more efficient tasks, discrete components of a new system can be better coordinated, and raw information can be more effectively manipulated to assist decision making (Crede and Mansell, 1998). This in turn results in more innovation, leading to a 'virtuous cycle' in which the initial adoption to new technologies snowballs into increased profits at the firm level and beyond.

3. Overcoming Geography: ICTs can overcome geographic boundaries, creating a more efficient global marketplace. As buyers and sellers are increasingly able to share information on process specification and delivery times, the production process can be spread across national boarders, and comparative advantage can be more efficiently realized. For developing countries, this can lead to larger markets and increased access to global supply chains.

4. Openness: Networking and information sharing also lead to demands for greater openness and transparency. Whether this means learning the true cost of a widget in Taiwan, the decision making process on a government agency, or the status of a central bank's foreign exchange reserves, ICTs are a powerful tool of empowerment. Thus ICTs might encourage the further spread and consolidation of democratic regimes.

While it is clear that knowledge and ideas play important roles in advancing economic and social welfare, it is important to recognize that the causal relationship is complex, and ICT is certainly not panacea. The enthusiasm with which the development community has rushed into ICT-related programmes often seems to overshadow the question of precisely how ICTs contribute to national development. Exclusive emphasis on ICT projects, at the expense of careful analysis and consideration of the broader economic, social and political elements that interact to improve the lives of individuals, is likely to result in unanticipated failures and wasted resources. Unfortunately, technological change moves so quickly that it often surpasses substantive analysis, leading to an over reliance on anecdotal evidence of justification for ICT projects. This in turn can lead to poor design programme and haphazard implementation schemes that do not account for local conditions, resulting in projects which fail to meet their objectives or may even harm the welfare of the supposed beneficiaries (Mansell, 1999, Fuchs, 1998). Furthermore, an investment in ICTs inevitably results in opportunity costs as they divert investments from other developmental needs and priorities.

Nevertheless, the revolution of ICTs has profound implication for economic and social development. The key issue for both governments and donors is to ensure that ICT access reaches even the most marginalized groups, while at the same time ensuring that ICT projects meet the needs and demand of the target population.

3.2 Trade and the Reduced Transaction Cost of Business

ICTs allow firms to spread component manufacturing across a wider array of countries, increasing the variety of service related activities that can be outsourced. This fosters efficient supply chain management and diversification and improves the logistics of moving goods and services across national borders. These factors have created new opportunities for large and small firms from developing countries to increase their sales range and tap into the global market for goods and services. The development of ICTs and the liberalization of national trading regimes could be a major factor in sustainable economic development (Hanna, et *al., 1996).*

The opportunities offered by the e-commerce revolution are particularly exciting. In 1999, global e-commerce revenues exceeded $150 billion and are predicted to climb as high as $3 trillion by 2003 (Forresters *Research, 1999). While the majority of e-commerce transactions still* take place within the industrialized countries, the economic and social implications of e-commerce for the developing world might be profound. The ability to reach a global audience, obtain instant market information and conduct electronic business transactions will increase economic efficiency and will open markets for goods and services from the developing world.

E-commerce is expected to benefit economic development in several ways; through allowing local businesses access to global markets, providing new opportunities to export a wider range of goods and services, and to improve the internal efficiency of developing countries' firms. First, e-commerce allows to business to reach a global audience. In Africa for example, the tourism and handicraft industries are realizing their ability to deliver their product information directly to the consumer. Tourist lodges, hotels, and government across the continent now maintain sophisticated websites advertising their unique features, handling booking orders, and promoting specials to interested consumers (Africa Business, 10/99).

Similarly, small manufacturers of traditional handicrafts are discovering how ICTs can assist the marketing and distribution of their wares. In Kenya, for, example, the Naushad Trading Company which sells local wood-carvings, pottery, and baskets, has seen an average revenue

growth from $10,000 to over a million in the year since it went online (Africa Business, 10/99).

A second opportunity created by e-commerce and its predecessor technologies is that ICTs can create digital marketplaces to manage supply chains and automate transactions, efficiency and opening previously closed markets to firms in developing countries. Because of this, global production processes are increasingly fragmented, with separate stages of manufacturing and value added taking place across national borders. Nowhere is this more apparent than in the information technology (IT) sector itself. The rapid obsolesce of new technologies has caused many IT firms to emphasize the development and marketing of new products, outsourcing physical production to more cost effective environments. This has created a comparative advantage for SMEs in developing countries, where lower cost of construction and quicker retooling create a more competitive manufacturing environment.

In Mexico, for example, the state of Guadalajara is experiencing a boom in indigenously owned and operated subcontractors that build components for major technology firms such as Compaq, Cisco Systems and IBM. Since 1994 electronics export from Guadalajara have increased to over $5 billion per year and the industry now employs over 60,000 workers, up from 5,000 in 1995 (Wall Street Journal, 3/2/2000). In this case a low combination of low labour costs, flexible subcontractors and geographical proximity to the US market has caused a boom in contract manufacturing with positive trade and developmental benefits. Similarly in 1998, Intel announced a plan to contract a $300million plant in Costa Rica to build next generation semiconductors forsaken in the United States. Costa Rica provided an attractive environment to Intel due to its stable economic and political conditions, well-educated and technologically savvy workforce, reasonable cost structure for labour, and other inputs, and a receptive investment environment- including favourable customs procedures and capital repatriation law (Spar, 1998).

ICTs not only open more trade in physical goods, they also present new opportunities for developing countries to benefit from trade in services. As new ICTs reduce the cost of information transfer, it is increasingly easy and cost effective to outscore information –intensive administrative and technical functions. Trade in service can be broken into two distinct categories: data entry and software development, in which firms parse the labour intensive aspects of information management and programme development to low cost environments, and back-office support such as inventory management, legal advice, accounting, marketing, distribution and research and development. Both areas have witnessed rapid growth

in recent years, as an improved communication network makes it easier and cheaper to outscore these activities.

The development of an indigenous Indian software industry is a good example of the developmental benefits that can result from expanding trade in services. Beginning as a low income environment for the labour-intensive aspects of writing software code, the country has been able to parlay that experience into the emergence of one of the most dynamic IT environments in the developing world. India now exports $5.7 billion in software products per year, and the sector may account for almost 25 per cent of the countries economic growth (*Business Week, 3/6/2000).*

A third benefit of e-commerce to developing countries is that it promises to revolutionize efficiency and the culture of business. While empirical data measuring efficiency and productivity related to e-commerce is scarce, anecdotal evidence suggests that business-to-business linkages have a number of discrete effects on global business practices. These include:

1. Better Infrastructure Communications: E-commerce applications make it possible for businesses to better coordinate different departments and systems. They open protocol standards of Internet applications and this makes it possible to connect processes such as logistics, manufacturing, and human resources that previously operated within closed environments. Thus business productivity and efficiency are increasing rapidly, leading to expanded profits and better market access to new and innovative companies.

2. Cost Savings: Electronic markets allow a more efficient mechanism for buyers and sellers to find each other and agree on a price. General Electric (GE) for example, operates the "Trade Process Network" which links it to suppliers and allows them to place electronic bid for component contracts. The system catalogues and displays the standards for each aspect of GE's parts requirement and allows suppliers to bid for contracts and receive payments electronically. The system has cut procurement cycles in half, processing cost by a third and the cost of goods purchased by 5 to 50n per cent (Economics,6/26/99).

3. Reducing Inventory Cost: Electronic interchanges can help firms better manage their inventories. This is particularly relevant in the age of "just-in-time" approaches to inventory management. Improving links between firms allows for better demand forecasting and control over the arrival of supplies, thus reducing inventory costs and lowering turnaround time. Dell Computers has led the way in

this process through a system linking its suppliers directly to its daily orders. As a result, parts arrive and are used on the same day in its manufacturing centers.

3.3 Capital Accumulation

Capital accumulation, whether foreign direct investment (FDI), portfolio flows, or domestic savings mobilization, is fundamental to economic growth and opportunity. ICTs are backbone of capital accumulation and management. In very few countries do banking systems still operate primarily through paper work and person-to-person interaction. Rather finance network has become digital and ICTs have allowed the expansion of banking services in developing countries to previously undeserved groups. In South Africa, for example, "Auto Bank E" has developed a fully automated savings system aimed at the poorest depositors. Customers can open an account with a deposit equivalent to only $8 (N1, 000) and benefit from a wide range of electronic banking services. All transactions are completed through automatic teller machines, which minimizes paper work and transaction cost in addition, the bank has used the data collection on depositors to analyze credit worthiness, resulting in much better credit access for the countries' poorest citizens. The system is very popular, with 2.6 million depositors and 50,000 more being added each month (Economist,3/25/2000).

ICTs not only improve the ability of the poor to access financial services, but are also central in attracting investment to economies. ICTs attract FDI in particular in three distinct ways:

1. Fist, the availability of advanced infrastructure, including modern communication network, is primary consideration in business calculations of where to invest. As communication cost continues to fall, geography and distance are increasingly less important factors in production site selection. Multinationals place a premium on environments that emphasize flexibility, responsiveness and adaptation to changing global markets. A recent survey of international firms in Hong Kong, Singapore and Taiwan, for example, found that the presence of advanced infrastructure was the most important consideration in the placement of regional headquarters, services and sourcing operations. It was the second most important factor in determining production siting (Mody, *1997).*

2. Second, ICTs attract high-tech industries seeking to service new and rapidly growing markets in the developing world and these invest significant recourses. Multinationals are moving quickly to position themselves for a predicted boom in consumer demand for computing

and telecommunications machinery in developing countries. Info-economy players such as Intel, IBM, and Motorola have moved briskly in Asia and now in Africa to established-commerce facilities, leading to plant investments throughout the regions. Dell Computers established a manufacturing plant in Malaysia in 1996 (Nain and Anvar, 1996) and opened the first foreign-owned personal computer (PC) manufacturing plant on mainland China in August 1999. In Brazil, sales of personal computers are growing at the rate of 30 per cent per year, which has attracted investment from companies ranging from Internet service providers (ISP) like America Online; software and marketing solutions such as Oracle and CommeceOne; and hardware producers such as Dell and Compaq.

3. Third, the process of privatizing state owned telecom companies and liberalization of the regulatory and tax environments in which they operate has also increased FDI into developing countries. Governments are increasingly seeking foreign partners to help modernize telecom infrastructure and bring desperately needed finance to moribund state-owned firms.

The lesson that an efficient ICT sector can attract investment is one that many developing countries such as India, Malaysia, Singapore, South Africa have move aggressively to improve ICT infrastructure and are becoming regional leaders in attracting FDI. Projects includes Malaysia's 420 billion multimedia super corridor, to India's liberalizations of trade regime for the high-tech sector in hopes of making it a cornerstone of future economic development to South Africa's 'Info.Com 2025' a program that brings together a diverse array of information and communication actors, to promote ICT development in addition to attracting foreign investment.

ICTs can also play an important role in attracting private portfolio and venture capital to developing countries in three ways:

a. First, the basis of market efficiency is access to information. Modern financial systems rely on computerized information processing and settlement mechanisms to move through global electronic networks. As a result, the world's financial markets have been integrated to an unprecedented degree. Broadly stated, ICTs have contributed to this trend by ensuring wider dispersion of market information to investors, reducing transaction costs in order-routing and execution systems, and increasing confidence in the supervision and regulation of emerging markets. For developing countries, the integration of ICT into equity and capital markets has resulted in improved access to a global pool of investment capital for industrial development as fund managers seek higher gains and reduced risk through portfolio diversification.

b. Second, a flourishing indigenous ICT sector attracts venture capital in much the same way it attracts FDI. Investors believe that the developing countries will witness a boom in IT spending and are seeking to export US style venture capitalism to emerging economies. Aggressive venture capitalists have been the major force in the US IT sector, bringing finance, business-plans, and know-how to high-technology firms. While most developing countries venture capital markets are a pool of available funds for entrepreneurs. India for example, is seeking portfolio and venture capital in the hopes of replicating Silicon Valley experience. Analysts expect India to attract upwards of 43 billion per year in venture capital from global investors including Softbank, Chase Manhattan, and GE Capital. In addition, India's wealthy expatriate community, particularly those that have succeeded in Silicon Valley, are increasingly seeking to bring both their expertise and accumulated wealth back to India (Red *Herring*,*22/2/2000).*

c. Thirdly and finally, ICTs also benefit a developing country's access to venture finance by improving risk management techniques. This process can benefit financial flows in the developing world in several important ways. First, the derivatives and forward contract can protect investors against exchange rate fluctuations. Multinationals with global supply chain can use these tools to reduce revenue volatility and allow better forecasting and planning. This in turn leads to investment decisions based upon the unique comparative advantage of a given location and parses of exchange rate movement to other investors. Second, business can use computer- modeled derivatives as well as forward contracts and options to protect themselves against commodity price fluctuation. Farmers in industrialized countries rely on well-developed markets in commodity futures and options to better ensure steady future profit flows. The spread of ICT into the developing world will likely enable a more efficient functioning of agricultural markets and boost profits in that sector. Third, firms, particularly banks, are increasingly able to manage different national regulatory and capital requirements through instant portfolio rebalancing, as well as software programs that automate risk profiles. This in turn increases efficiency and allows finance to flow into regional areas and sectors that may otherwise present an unattractive investment profile (Economist, 11/12/99).

4.0 CONCLUSION

The worldwide development of information and communication technology (ICT) has accelerated dramatically over the past decade,

spurred by increasingly global economy. For many observers the global economy is entering digital age and information has become a primary resource for economic development. The developing countries are not left out in this global revolution of business processes by ICTs. This is because those countries without access to latest (and more expensive) tools and technologies will find themselves unable to compete in the global marketplace.

Again, despite the seemingly challenges confronting the full adoption of ICT in global business it is imperative that ICT has come to play a very significant role in global economic development.

5.0 SUMMARY

In summary, this unit on ICT and Economic Development has the following as the major points to be considered:

- Perhaps the simplest way of demonstrating the importance of ICTs in the development process is to examine the willingness of the poor to pay for service.

- While it is clear that knowledge and ideas play important roles in advancing economic and social welfare, it is important to recognize that the causal relationship is complex, and ICT is certainly not a panacea.

- Nevertheless, the revolution of ICTs has profound implication for economic and social development.

- ICTs allow firms to spread component manufacturing across a wider array of countries, increasing the variety of service related activities that can be outsourced. This fosters efficient supply chain management and diversification and improves the logistics of moving goods and services across national borders.

- ICTs not only open more trade in physical goods, they also present new opportunities for developing countries to benefit from trade in services.

- Capital accumulation, whether foreign direct investment (FDI), portfolio flows, or domestic savings mobilization, is fundamental to economic growth and opportunity. ICTs are backbone of capital accumulation and management.

- ICTs not only improve the ability of the poor to access financial services, but are also central in attracting investment to economies.

• ICTs can also play an important role in attracting private portfolio and venture capital to developing countries.

• The spread of ICT into the developing world will likely enable a more efficient functioning of agricultural markets and boost profits in that sector.

6.0 TUTOR-MARKED ASSIGNMENT

1. In what ways does ICT help the development process?
2. Discuss the relationship between Capital Accumulation through ICT and Development.

7.0 REFERENCES/FURTHER READINGS

Odukoya, Atinuke (2005). Engendering the Information Society in Nigeria. Women Magazine, DevNet. Publication.

Zhen-Wei Jiegn, Christien et al; "Contribution of ICT to Economic Growth". World Bank Working Paper, No 24, 2004.

Zhen-Wei Jiegn, Christien et al; "Factors Influencing the Contribution of ICT to Economic Growth". World Bank Working Paper, No 24, 2004.

Grace, Jerry et al; "ICT and Broad Based Development". World Bank *Working Paper, No 12, 2004.*

UNIT 4 INTRODUCTION TO COMPUTERS 1

CONTENTS

1.0 INTRODUCTION

There are several definitions associated with the computer. For the purpose of introduction, we will define the computer as a fast operating, versatile machine that can be used for home and business tasks to enhance productivity. In other words, a computer is a collection of electronic parts or hardware, that have a set of electronic instructions called software. All computers perform the same basic functions: they enable you to store and manipulate information.

Whilst it is true that computers can be used very effectively to perform all kinds of tasks, particularly now they are available at prices most organizations can afford, it is all too common to find examples where computers have been introduced to make things better and have only made things worse. The reason for this is quite simple: a computer will only succeed where those using it have taken the trouble to determine

1. What they require the computer to do
2. How the computer can best do it
3. Whether the benefits are worth the costs
4. Whether those involved are ready, willing and able to work with the computer.

What is a personal computer? Personal computers, or microcomputers, are often called PCs. This is because a PC often stands alone on your desk, complete with all the equipment you need to perform your tasks. However, PCs do not have to stand-alone. A network can link them in order to share information and equipment with other users.

How did computes become popular? International Business Machine (IBM) introduced its first personal computers, the IBM PC. Other companies began making and selling computers that looked and worked like the PC. These copies are called IBM-compatible, PC-compatible, or clone systems.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- describe and identify a computer
- enumerate the basic characteristics of a computer
- make the computer to work for you
- differentiate the classes and types of computers
- differentiate the types of personal computers
- enumerate the functions of computers
- state the benefits associated with computers in the work place

3.0 MAIN CONTENT

3.1 The Characteristics of a Computer

Computers display the following characteristics to a greater or lesser extent depending on their type and application:

1. The ability to perform calculations at very high speed
2. The ability to take in information and to store that information for future retrieval or use
3. The ability to take in and store a sequence of instructions for the computer to obey. Such a sequence of instructions is called a program and must be written in the language of computer
4. The ability to obey a sequence of program instructions provided the program is stored within the compute
5. The ability to use simple logical rules to make decisions for their own internal control, or for the control of some external activity e.g. to take over the role of the calculator operator
6. The ability to communicate with other systems
7. The ability to exploit a complex internal structure of a microelectronic circuitry in a variety of ways.

3.2 Classes and Types of Computers

Classes of Computers

There are two classes of computers; analog computers and digital computers.

Analog Computers: This class of computer are special purpose machines that surfaced in the late forties (1948). They are used solving scientific and mathematical equations or problems. An example is the thermal analyzer. Data and figures are represented by physical quantities such as angular positions and voltage.

Digital Computers: They are machines made up of combinations of chips, flip-flops, buttons and other electronic devices to make them function at a very fast speed. A digital computer has its numbers, data letters or other symbols represented in digital format. They are mostly

special purpose machines unless minor specifications are included in the design.

A computer that combines the features of a digital and analog computer is called a hybrid computer.

Types of Computers

In classifying computer into types we start from the third generation computers made in the 60s, (excluding the first and second generation computers of the 40s). Basically there are 5 types of computers:

1. Super Computers

A super computer is the most powerful computer available at any given time. These machines are built to process huge amounts of information and do so very quickly. Supercomputers are built specifically for researchers or scientists working on projects that demand very large amounts of data variables; an example is in nuclear research, where scientists want to know exactly what will happen during every millisecond of a nuclear chain reaction. (To demonstrate the capability of super computers, for an air pollution control project that involves more than 500,000 variables, it will take a mini computer about 45 hours to complete the simulation process while it will take a super computer 30 minutes only). They are big in size, generate a lot of heat and are very expensive. (Super computers are made by CRAY Company).

2. Mainframe Computers

The largest types of computers in common use are the mainframe computers. They are designed to handle tremendous amounts of input, output and storage. They are used mainly by large organization like the PHCN, NITEL, and CBN. Other users access mainframe computers through terminals. Terminals consist of a type of keyboard and a video display i.e. monitors. The mainframe is usually in the computer room (Mainframe computers are made by IBM, Boroughs & Univac).

3. Mini Computers

These are physically small compared to mainframes and are generally used for special purposes or small-scale general purposes. The best way to explain the capabilities of mini computers is to say they lie between mainframes and personal computers. Like mainframes, they can handle a great deal more input and output than personal computers. Although

some minicomputers are designed for a single user, many can handle dozens or even hundreds of terminals. Advances in circuitry means modern mini computers can out-perform older mainframes of the 60s. (Examples are Digital Equipment Company's PDP II and Vax rang)

4. Workstations

Between mini computers and micro computers – in terms of processing power is a class of computers known as workstations. A workstation looks like a personal computer and is typically used by one person, although it is still more powerful than the average personal computer. The differences in the capabilities of these types of machines are growing smaller. They significantly differ from micro computers in two ways: the central processing unit (CPU) of workstations are designed differently to enable faster processing of instructions and most of the micro computers can run any of the four major operating systems. Workstations [(Reduced Instruction Set Computing (RISC)]use UNIX operating system or a variation of it. (A note of caution: Many people use the term workstation to refer to any computer or terminal that is connected to another computer. Although this usage was once a common meaning of the term, it has become out dated) (The biggest manufacturers of workstations are Sun Microsystems).

5. Micro Computers/Personal Computers

The term microcomputers and personal computers are used interchangeably to mean the small free- standing computers that are commonly found in offices, homes and classrooms. Many micro computers are built specially to be used in watches, clocks, and cameras. Today, PCs are seriously challenging mainframes and mini computers in many areas. In fact today PCs are more powerful than mainframes of just a few years ago, and competition is producing smaller, faster models every year.

Types of Personal Computers

There are different types of PCs depending in the size adaptability, portability and convenience.

a. THE DESKTOP: This is the first type of PCs and the most common. Most desktops are small enough to fit on a desk, but are a little too big to carry around.

b. THE LAPTOP: They weigh about 10pounds (4.5kg). They are battery – operated computers with built–in screens. They are

designed to be carried and used in locations without electricity. Laptops typically have an almost full –sized keyboard.

c. THE NOTEBOOK: They are similar to laptops and PCs, but smaller. They weigh about 6 to7 pounds (2.7 – 3.2kg). As the name implies, they are approximately the size of a notebook and can easily fit inside a brief case.

d. THE PALMTOP: They are also known as personal digital assistance (PDAs) and are the smallest of portable computers. Palmtops are much less powerful than notebooks or desktops models and feature built-in applications such as word processing. They are mostly used to display important telephone numbers and addresses.

3.3 Functions of Personal Computers

Personal computers can do a lot of things. The most common tasks computers perform include:

a. Writing documents such as memos, letters, reports and briefs
b. Budgeting and performing accounting tasks
c. Analyzing numeric information
d. Searching through lists or reports for specific information
e. Scheduling and planning projects.
f. Creating illustrations
g. Communicating by using electronic mail
h. Advertising products and services.

3.4 The Importance of Computers in Business and Organizations

Computer technology has revolutionized businesses and organizations all over the world. Virtually every company, large or small, now relies on information processing equipment to automate or assist all aspects of commerce. Computers are essential in meeting the challenges of meeting global competitiveness, where business must be efficient and responsive, and must produce high-quality goods and services at an ever lower cost. Without computers to produce accurate up-to-the-second information needed to produce strategic decisions and to manage production processes, many businesses and organizations will find it impossible to survive.

Computers have become so important to most corporations that extensive precautions are taken to ensure that systems and data will be available at all times.

Computers are used primarily to collect, manage and reproduce a wide variety of information for business and organizational data. That can mean everything from educational to financial records to lists of parts to make things and plans for new products.

Computers do more than keep track of things; they help people to make better decisions. Computers use stored information to construct simulations ranging from simple "what-if" analyses to realistic depictions and animation of new products. Many workers spend a good portion of their days using computers to predict the effects of simple business decisions.

Computers also help people to communicate- both directly and indirectly. Publishing software brings the power of the press within the reach of everybody. Office employees today use electronic mail to stay in touch with their co- workers.

Personal computers have empowered people in ways that creators of these machines never envisioned. In the process, computers have caused and continue to cause major cultural changes in many businesses. They have liberated organizations from bureaucratic information system management.

Computers in the Corporate Environment

Our society and culture are heavily influenced by how we spend our time. Most people spend from one-third to one-half of their lives working, and the companies that employ most of us range in size from large international corporations to small businesses. Given this, we should look at how these organizations use computers. In this section, we will look inside business – at what some of the departments and people within companies do, and how they might use computers, both collectively and individually.

1. Finance and Accounting

Of all the areas in business that use computers, none relies on them more heavily than finance and accounting departments. From staff accountants to chief financial officers, practically every area of finance is saturated with computers. The software applications that finance personnel use with their computers also run the gamut of the software industry.

Because businesses are unique in some ways and common in other ways, accounting software is sold modularly. At the heart of every

accounting system is the general ledger, but that is only the core of an accounting system. An accounting system helps accountants to keep track of financial statements. Financial transactions include sales of the company's products or services, purchases of supplies and inventory from supplies, employee payroll payments, and even agreements that a company enters into where there is no immediate transfer of money or obligations.

As you might imagine, keeping track of so many highly detailed transactions would be an overwhelming task without the help of computers. Even with computers, setting up a system to capture all the important information reliably is a daunting task. The approach that accountants and software developers take is to classify and capture transactions according to their sources. This way, data can be checked and validated before they are dumped into the general ledger, where they are summarized again and used to produce financial statements. The first modules many companies add to a general ledger package is generalized programs to manage account receivable and account payable.

2. Retail Sales

How many times have you gone into a retail store and purchased items at the checkout counter from a clerk with a computerized cash register? In the vast majority of stores, these computerized cash registers are tied directly into the company's accounting system. In fact, they are not called cash registers any more. Today they are called point-of-sale **(POS) terminals. Every time the salesclerk scans an item, the terminal** looks up the price and description in the company's central computer (accounting) system, and when the sale is completed, each item is removed from the inventory records. For a retail store, the point of sale is the main entry point for transactions on the accounts-receivable side of the books.

3. Wholesale

One of the many products that 3M Corporation manufactures is diskettes for computers. 3M sells vast numbers of diskettes to computer manufacturers and software companies to distribute their software. In addition, 3M sells diskettes to distributors who resell them to computer and office-supply stores around the world. The sale transaction that an employee at 3M goes through is similar to the transaction the point-of-sale clerk performs at a terminal. The major difference is that the wholesale salesperson needs to use a computer terminal to check stock, to schedule a shipping date, and to get billing information, instead of collecting cash or a check.

4. Shipping and Receiving

Warehouses store finished goods inventory (products that are ready to be sold), as well as raw materials, in the case of a manufacturing company. The shipping docks are the center of control for a warehouse; today, warehouse employees almost always use computers extensively. Some of the most important transactions actually take place as goods are shipped and received.

When the salesperson makes a sale and schedules a shipment date, that information makes its way to the warehouse floor on the day the goods are scheduled to ship, and is also used to determine when stock should be reordered. Although goods are earmarked when a sale is made, an accounting transaction doesn't take place until the goods are physically loaded onto a truck and driven away. When products are shipped, the warehouse employee enters the event into the computer system, which creates the accounting transaction.

5. Manufacturing

In manufacturing departments, managers use the computer to schedule production of products or components. Their instructions to produce finished goods result from the orders booked by the sales department, as well as from strategies in the minds of top-level management that may call for increased inventory levels for products.

Manufacturing managers use computers and a technique called **materials requirement planning (MRP) to ensure that the materials** needed to produce products will be available as they are needed in the manufacturing process. Raw materials and components are carefully scheduled to arrive when they're needed, but not too long before they're needed. Excess materials in storage waste not only production space, but also company resources to pay for the materials before they are needed.

6. Purchasing

The purchasing department is charged with buying materials and components for production, as well as capital equipment. Purchasing employees are charged with acquiring goods and services for a company at the most favorable pricing and terms possible.

For production materials and components, purchasing must be highly coordinated by production or manufacturing departments, to ensure that needed materials arrive when they're needed and not too far in advance.

Purchasers arrange for the delivery of goods and schedule the arrival times in the central computer system. Just as sales are not final until the product is shipped, though, purchases are not final until the goods are received at the receiving dock.

7. Personnel and Human Resources

Computer technology has allowed the field of human-resources management to become more efficient than ever before. Especially in large companies, computers can help the human resources managers to make more informed decisions about which candidates to hire, and once these people are aboard, to see that the employees receive all the training and orientation that they need.

Human-resources management systems are usually based on database software that provides quick access to employee records and history. Using these systems, human resources managers can ensure that employees receive their scheduled performance evaluations and are considered for promotions and wage increases when they are supposed to be.

Computers in Small Businesses

Small businesses have all the elements of large businesses. The major difference is that there are fewer people, so the employees of a small business have to be able to wear more hats than their counterparts in the corporate environment. This makes it even more important that each team member be flexible and knowledgeable about the organization's computer system. Whereas large corporations still make extensive use of mainframe and mini computer systems, small businesses usually rely completely on PC networks.

4.0 CONCLUSION

Beginning from the advent of computers in the 1960s till today, the computer has come to stay as the major tool used for the drive of the information and communication technologies of the 21st century.

Without computers the role played by ICT in globalizing business and transaction would not have been possible. An understanding of the trend in terms of types and categories, as well as the benefits of computers in the work place strengthens your crave for its applications.

5.0 SUMMARY

- We have defined the computer is a fast operating, versatile machine that can be used for home and business tasks to enhance productivity. In other words, a computer is a collection of electronic parts or hardware, that have a set of electronic instructions called software. All computers perform the same basic functions: they enable you to store and manipulate information.

- Personal computers or microcomputers are often called PCs. This is because a PC often stands alone on your desk, complete with all the equipment you need to perform your tasks.

- The computer has the ability to take in and store a sequence of instructions for it to obey. Such a sequence of instruction is called a program and must be written in the language of computer.

- A super computer is the most powerful computer available at any given time. These machines are built to process huge amounts of information and do so very quickly.

- The term micro computers and personal computers are used interchangeably to mean the small free- standing computers that are commonly found in offices, homes and classrooms.

- Personal computers can do a lot of things. The most common tasks computers perform include writing documents such as memos, letters, reports and briefs.

- Computer technology has revolutionized businesses and organizations all over the world. Virtually every company, large or small, now relies on information processing equipment to automate or assist all aspects of commerce.

- Of all the areas in business that use computers, none relies on them more heavily than finance and accounting departments.

- Computer technology has allowed the field of human resources management to become more efficient than ever before. Especially in large companies, computers can help the human resources managers to make more informed decisions about which candidates to hire and once these people are aboard, to see that the employees receive all the training and orientation that they need.

6.0 TUTOR-MARKED ASSIGNMENT

1. Briefly discuss the roles of computer for accounting and finance functions in an organization
2. Mention 5 characteristics of a computer.

7.0 REFERENCES/FURTHER READINGS

Anderson, R.G (1994). Data Processing: Principles & Practice, Vol. 1. Pitman Publishing.

Anderson, R.G (1994).Data Processing: Information Systems & *Technology, Vol. 2. Pitman Publishing.*

French, C.S. (1993). Computer Studies. DP Publishing Ltd.

Norton, P (1995). Introduction to Computers. Macmillan/McGraw-Hill.

Ron, W. (1995). How Computer Works. Macmillan Computer Publishing.

UNIT 5 INTRODUCTION TO COMPUTERS 2

CONTENTS

2.0 OBJECTIVES

At the end of this unit you should be able to:

- identify the various parts of the personal computer
- identify and differentiate the various types of computer devices
- identify input devices and state their types and uses
- identify processing devices and state their types and uses
- identify storage devices and state their types and uses
- identify output devices and state their types and uses.

3.0 MAIN CONTENT

3.1 Components the Personal Computer

A personal computer is not a single unit. A typical computer consists of several basic parts or components that work together. To perform any computer task you need two major components: the hardware and the software.

The hardware is the physical components of a computer system. Generally you can think of the hardware as any part of the computer that you can see or touch. Although the hardware of a computer is capable of performing marvelous tasks, it cannot accomplish any of them without the vital instructions that the software provides.

The software is a set of instructions that tells the hardware what to do. You can't see or touch the software, although you can see packages that contain the software. It is typically distributed on CD-ROM disc and is installed on the computer hard drive.

The major hardware components of the personal computer consist of the following:

- The System Unit: This is the part of the computer where data is processed, memorized and stored to produce information. It is the central part of the computer, i.e. the engine room of the computer. Generally any device attached to the system unit is considered peripheral.

- The Keyboard: It is used for entering commands and data.

- The Mouse: This is for entering command and data and to select icons on the monitor.

• The Printer: It is for transferring work to paper, i.e. to print copies of documents created using the computer.

NOTE: You don't need a printer to be able to run a computer.

3.2 Input Devices

Input devices are the computer hardware that accepts data and instructions from a user. Input devices have been built in many forms to help in communicating with the computer. The most common input devices are the keyboard and the mouse.

1. **The Keyboard: The keyboard of the personal computer comes in** a number of styles. The various models may differ in size and shape, but except for a few special purpose keys, MDS keyboards are laid out almost identifiably. The most common keyboard used today was established by IBM. The computer keyboard is more than just a typewriter. It contains all of the keys required for typing letters, numbers, plus the keys for entering commands and moving around on the screen. There are 101 keys arranged in groups: Alphanumeric, Numeric, Function and Arrow/Cursor movement keys, and Computer keys.

2. **The Mouse: The mouse was first used in the mid 80s and first** gained widespread recognition when it was first packaged with Apple Macintosh.

A mouse is a pointing device that enables you to quickly move around on the screen, and to select commands from menus rather than type the commands. A mouse is useful because it enables the user to point at items on the screen and click a button to select the item. It is convenient for entering certain data.

The mouse is connected to the computer by a cable or tail. The cable attaches to either a serial port or a special mouse port. On top of the mouse are buttons. Usually, there are two but sometimes there are three. The buttons are used to activate objects on the screen. Everything you do with the mouse you accomplish by combining pointing with three basic techniques - clicking, double-clicking and dragging.

There are four types of mouse:

• The serial mouse is connected to the serial bus.
• The bus mouse comes with a special electronic card that slides into one of the expansion slots inside the computer. One edge of this card

attaches to the back of the computer, providing a special port just for the mouse.

- The mechanical mouse has a ball inside of it that extends just below the housing of the mouse itself.
- The optical mouse has no moving part at all. Instead of a ball, it has a built-in photo detector that senses the movement of the mouse over a special pad with gridlines printed on it.

3. **Track Balls: A trackball is an input device that works like an** upside-down mouse. You rest your hand on the exposed ball and the fingers on the button. To move the cursor around the screen, you roll the ball with your thumb. Trackballs are much popular with notebook computers. They require less desk space than the mouse.

4. **The Joystick: This is a pointing device commonly used for** games. It is not used for business applications.

5. **The Pen: It is an input device that allows a user to write on or** point at a special pad on the screen of a pen-based computer, such as a personal digital assistant (PDAS).

6. **The Touch Screen: A computer screen that accepts input** directly into the monitor; users touch electronic buttons displayed on the screen. It is appropriate in environment where dirt or weather would render keyboards and pointing devices useless.

7. **The Scanner: This is an input device used to copy images into a** computer memory without manual keying. It works by converting any image into electronic form by shinning light on the image and sensing the intensity of reflection at every point. There are several kinds of scanners. These includes: hand held, flatbed, and sheet-feds.

8. **The Bar-Code Reader**
   This is one of the most commonly used input devices after the keyboard and mouse. It is commonly found in supermarkets and department stores. This device converts a pattern of printed bars on products into a product number by emitting a beam of light-frequently from a laser that reflects off the bar code image. A light sensitive detector identifies the bar-code image by special bars at both ends of the image. Once it has identified the bar code, it converts the individual bar patterns into numeric digits.

3.3 Processing Devices

Basically two components handle processing in a computer: the central processing unit (CPU) and the memory.

1. The Central Processing Unit (CPU)

The central processing unit (CPU) is a tiny electronic chip known as the micro processor located in the system unit. It is installed on the main circuit board of the computer, the motherboard. The CPU as the name implies is where information is processed within the computer. In this regard, you might think of the CPU (processor) as the brain of the computer. The CPU is otherwise known as microprocessor.

Information constantly flows back and forth between the CPU and all the other parts of the computer. The CPU is in the middle controlling the flow of information. The CPU also calculates numbers when required

The amount of data that a chip receives at one time and the amount of data that leaves the chip is a measure of the chip's processing capability. In addition to receiving and sending data, chips internally process data.

Every CPU has at least two basic parts. The control unit and the Arithmetic Logic Unit (ALU). The control unit coordinates all the computer activities and contains the CPUs instruction to carry out commands. The ALU is responsible for carrying out arithmetic and logic functions. In other words, when the control unit encounters an instruction that involves arithmetic and logic it refers it to the ALU.

2. Memory

What happens to all the information we put into the computer: before, while and after information is processed? It is held in the computer memory or Random Access Memory (RAM). The memory to which we are referring here is not the kind of long-term storage that allows you to save work on a floppy disk and months later to use it, but rather a short term holding area that is built into the computer hardware.

How the Memory Works: While the CPU is fast and efficient, it cannot remember anything by itself. It often refers to the memory in the computer for software instruction and to remember what it is working on. The term RAM and memory are often interchangeable. RAM refers to the way the CPU searches through memory for the information it needs.

For the workings of a memory, information is stored in memory chips. The CPU can get information faster from RAM than it can from a disk. A computer then reads information or instruction from disks and stores the information in the RAM where it can get the information quickly. The CPU processes the information and then returns to the RAM.

Note that memory is temporary because memory chips need electricity to hold information. If power is interrupted, information in memory is lost forever.

Measuring Memory: Memory is measured in a small group of data called bytes. Each byte consists of eight bits. The byte is the basis of all measures dealing with the computer. Because each byte is very tiny, other terms are often used to measure larger amounts of memory. Memory measurements are in hundreds, thousands, millions and billions.

Byte: one character (letter, number space or punctuation mark)
Kilobyte (k): one thousand bytes =1,024 bytes
Megabyte (MB, Meg. or M): one million bytes = 1,048, 576 bytes
Gigabyte (GB): one billion bytes = 1,073,741,824 bytes.
1024 Gigabyte = 1 Terabyte
1024 Terabyte = 1 Petabyte
1024 Petabyte = 1 Exabyte
However for convenience, these values or figures are rounded up to zeros. For example 1 kilobyte though is actually made of 1024 bytes; it is often rounded up to 1000 bytes.

3.4 Storage Devices

Among the most important part of a computer system are the devices that allow you to save the product of your labour. The physical components or materials on which data are stored are called storage media. A storage device is a piece of hardware that permanently stores information. Unlike electronic memory, a storage device retains information when electric power is turned off.

How Data is Stored: Two technologies are used to store data today; they are the magnetic and optical storage. Although devices that store data typically employ one or the other, some combine both technologies. The most common storage devices use magnetic technology. For example floppy disk and hard disk use magnetic technology while CD-ROM and WORM (Write Once Read Many) use optic technology.

Storage Device Names: Storage device names are designed to instruct the computer to save information to specific drives. The drives are named after letters of the alphabet. On most computers, the drives are configured as follows:

Drive A: For floppy disk

Drive B: Usually below Drive A also for the floppy disk.
Most computers have only one floppy disk drive (Drive A), in which case there is no drive B.

Drive C: For the hard disk drive which is usually inside the system unit.

Drive D: For CD-ROM drive.

Types of Storage Devices: Disks are the most commonly used types of storage device. Two forms of disks for storage are floppy disk and hard disk.

In general, floppy disk and hard disk / drives are similar in their construction and operation. The most obvious differences between the two types are that the floppy- disk is visible, the hard disk is not. The floppy disk drive is designed to receive removable floppy disk.

The hard disk consists of several inflexible metal platters that stay within the housing. The hard disk can store more information and process information faster. Because of this difference, hard drives and floppy drives are used in different ways. Some storage manufacturers provide another type of device that combines some of the benefits of floppy disks and hard disks – the removable hard disk.

There are several storage devices and primary among them are:

1. The Floppy Disk: The floppy disk is a circular flat piece of plastic made of a flexible (or floppy) magnetic material on which data are recorded. Floppy disk drives store data on both sides of the disks. Earlier computers stored data on only a single side of the floppy disk. Floppy disks are commonly used for:

a. Moving files or data or information between computers not connected through communication hardware, i.e. portability.

b. Loading new programmes unto a system: Although extremely large programmes are available on CD-ROM or tape, some programmes are also sold on floppy disk.

c. Backing up data or programmes, the primary copy of which is stored on a hard disk. Backing up is the process of creating a duplicate set of the hard disk's programmes and data for safekeeping.

Types of Floppy Disks: There are two physical sizes; 5 ¼ inch and 3 ½ inch. The size refers to the diameter of the disk, not the capacity. A 3 ½ inch floppy disk, high density, can hold 1.44 MB data. The 5 ½ inch floppy disks come in two capacities, double density and high density. The 3 ½ inch comes in three capacities; double density, high density and very highly density. The density is a measure of the quality of the disk surface. The 3 ½ inch disks are more durable and as a result the 5 ¼ inch has almost disappeared.

Taking Care of Floppy Disks: The disk includes a sturdy plastic case and a metal covering to protect the media from finger marks, scratches, and dust. However, you still need to take precautions when handling disks. For example:

- Store disks in a disk file box to protect them from dust
- Store disks in a cool, dry place to avoid exposing them to water, direct sunlight, or heat from vent.
- Keep disks away from magnets
- Do not send disks through the metal detectors at airport security gates. This can affect floppy disks. Request that they be inspected manually.
- Never force a diskette into a disk drive and never remove a disk from a drive when the light is on.
- Always label your diskette to avoid a mix up.
- Do not slide the cover back on 3.5-inch disks, and do not touch the recording medium on any disk.

Write Protecting a Floppy Disk: To protect the contents of a disk from being accidentally erased or modified you can write – protect the disk. This allows the computer to read data from the disk, but not change it. You can turn a disks write-protection ON and OFF as many times as possible.

Floppy Disk Formatting and Capabilities

The different capacities of disks are generally a function of the number of sides, tracks and sectors per track. The capacity of an individual disk is determined when the disk is formatted. Formatting prepares the disk's surface to hold data. Every process of mapping a disk is called formatting or initializing the disk. Every new floppy disk must be

formatted. However, you can buy floppy disks that have been preformatted for your particular computer.

When you format a disk, the disk drive divides the surface area of the disk into concentric tracks or circles and wedge-shaped sectors. This type of storage unit makes it easier for the computer to locate files.

Hard disks are capable of storing much data than floppy disks and they tend to store and retrieve data much more quickly than floppy disks. Because of these characteristics, hard disks are well suited for storing files that:

- are large
- must always be available to the computer such as operating system files or application; and
- require quick access.

2. The Hard Disk: **The hard disk is generally not visible because hard** disks are usually enclosed within the system unit. The hard disk is a stack of metal platters that spin on one spindle like a stack of rigid floppy disks. Unlike floppy disks where the disk and drive are separate, the hard-disk drive, or hard drive is the whole unit. Generally you cannot remove the hard disk from its drive; however some manufacturers make removable hard disks that plug into a separate drive unit.

Hard disks come in several sizes. The size of the hard disks is measured in terms of the size of the platter. The different sizes of hard drives available are 2.5”, 3.5”, 5.25”, etc. A 2.5 inch disk is specifically designed for a small computer.

On the other hand, the number of programs and the amount of data that a hard disk can store is measured in megabytes. The capacity of the drive is the single most important consideration in its selection. There are no standard capacity sizes for hard disks; they typically hold 4 G or more data.

3. The CD-ROM: CD-ROM disks is hard, plastic, silver – a coloured disk. CD-ROM is an acronym for Compact Disc Read – Only Memory. This implies that the disk can only be read. You cannot change or overwrite the contents of a CD-ROM disk.

CD-ROM disks provide tremendous storage capacities. A single CD-ROM disc can store up to 680 MB of data, sound, and video. This is equivalent to 485 floppy disks.

Like a floppy or hard disk, data is stored on a compact disc by using a series of 1s and Os. Os are represented on the disk by using flat surfaces, and they are represented by pits in the surface. To read data on the disc, the CD-ROM drive uses a laser bean to reflect light off the disc surface. The pitted areas of the disc reflect light differently from the level areas, which let the drive differentiate between 1s and 0s.

Uses of CD-ROM:CD-ROM disks are appropriate for multimedia: the combination of several forms of media (text, sound, video and graphics) to present information.

4. Tape Drives: A tape drive is a device that reads and writes data to the surface of a magnetic tape, generally used for backing up or restoring the data of an entire hard disk.

The best use of tape storage is for data that you don't use very often. It thus becomes useful to back up hard disks because the disk are vulnerable to change and can fail. Tape drives unit provides a quick convenient way to back up a hard drive. The tape enables you to copy files from your hard disk to a cassette tape for protection. If anything happens to the data or profanes on your hard disk, you can restore them from the tape.

To make a back up tape, you insert a tape cartridge into the tape drive. Tapes must be formatted before you can use them. To save time you can buy tape cartridges already formatted. Be sure to use a tape cartridge that is large enough to store more information than you are backing up to avoid having to exchange cartridges during the backup process.

5. The Zip Drive

Zip drives are an alternative to tape back up units or tape drives. A zip drive can be internal or external. Zip drives have removable cartridges or disk. A zip drive holds about 100MB to 250 MB of Data.

3.5 Output Devices

Output devices return processed data, that is, information back to the user. In other words, output devices allow the computer 'talk' to us. The most common output devices are the monitor and the printer. Others include modems and speakers.

1. The Monitor: The monitor is an output device that enables the computer to display to the user what is going on. It has a screen like that of a television. It is commonly referred to as the screen or display. It is the main source for output of information from

the computer. As data is entered through an input device, the monitor changes to show the effects of the command. Messages displayed on the screen allow the user to know if the command is correct.

Features of the Monitor

(a) SHAPE: Two basic shapes of monitors are used with micro computers

(i) The Round Monitor: This type uses CRT (Cathode Ray Tube).This is the typical monitor that we see on a desktop computer. It looks like a television screen.

(ii) The Flat Panel Monitor: This type uses liquid crystal (LCD's) to render images and is commonly used with notebooks.

(b) SIZE: It is measured in inches diagonally across the screen. The majority of computers are sold with 14-inch monitors. They are economical and the size is adequate for most uses. However, for more serious applications, large monitors (17" 21") have certain advantages: they provide more room for icons, tools, windows etc.

(c) ANTI-GLARE: This is coated glass fixed to a monitor to reduce reflections and make viewing much easier.

(d) STANDS: Some monitors have tilt and swivel that make viewing easier.

(e) CONTROL: These are controls to adjust the brightness and contrast

(f) COLOUR: There are basically two types; monochrome i.e. only one colour is displayed against a contrasting background usually black. Or coloured, which displays multiple colours.

(g) THE VIDEO ADAPTER CARD: This is a piece of hardware that controls a monitor. It is built into the computer's motherboard or installed as an expansion card. It has its own memory, which is separate from the computer's in-built memory. That way the video adapter card can build graphic images without using computer memory needed by the system and programmes. The amount of memory installed on the video card determines the number of colours to be displayed.

2. The Printer: The printer is an output device that produces on hard copy or a print out on a paper i.e. It takes data from its electronic form and prints it out on paper. There are three principal types of printers; Laser, Inkjet and Dot – Matrix. In evaluating these types, 4 criteria are most important:

a. Image quality
b. Speed
c. Noise level
d. Cost (printer and accessories)

LASER PRINTERS: Laser printers are much more expensive than other types of printers; their print quality is higher. They are also much faster and are very quiet. As the name implies a laser is at the heart of this printer. A separate computer is built into the printer to interpret the data that it receives from the computer, and to control the laser. A laser beam is moved by using a moving mirror to create an electrical charge on a rotating drum. The electrical charge attracts a dry ink substance called toner. The toner is melted onto the page to leave a permanent high-quality image.

Laser Printer speeds are often rated in "pages per minute" or ppm. Typically, the higher the value, the faster the speed. The complexity of the pages you are printing determines how fast the printer prints. Laser printers use the measure of dots per inch (dpi) to determine print quality. Laser printers vary, generally ranging from 300 to 1,200 dpi.

INKJET PRINTERS: These printers are less expensive than laser printers and they produce high quality printouts quietly; however they are slow. Inkjet printers are necessary when you need shop laser-quality text. However, to print graphics inkjet printers cannot produce the same quality output as laser printers. Typically, an inkjet printer is more expensive than a dot matrix printer but costs about half as much as a laser printer. They are portable and sleek, and were developed to be used with notebook computers. In addition inkjet printers are the best option if you want a good resolution colour printer. Just like laser printers, inkjet printers have their own memory different from the memory of the computer.

Inkjet printers work by creating an image on a paper when print head ink passes through many tiny holes known as nozzles. Each nozzle heats up the liquid ink which bubbles and when the bubbles burst, droplets of ink are sprayed onto the page.

How Inkjet Works: Inkjet printers offer two modes: draft mode (which is faster and uses less ink) and high quality mode.

DOT MATRIX PRINTERS: Dot-matrix printers were the first type of printers commonly used with personal computers. They are generally the least expensive and the most versatile; however they are slow and noisy. The print quality is less than that of Inkjet printers. Dot-matrix printers can handle multi-part forms such as invoices and carbons.

Dot-matrix printers create graphics and characters as a collection of tiny dots. They work by impact; tiny pins inside the print head hit the printer ribbon against the paper, forming the characters and pictures.

Dot-matrix printers remain popular because they are perfectly suited for some jobs especially multi copy forms such as invoice and forms which rely on impact to transfer printer characters from one copy to the next.

Choosing a Printer: Choosing the right printer involves the following considerations:

(i) What quality does your printing require?
(ii) How fast do you need your printing?
(iii) What type of paper do you have to print?
(iv) What is the cost of the printer and consumables?

3. The Sound Card: Sound Cards, otherwise known as soundboards, is a hard ware board. It is a device that produces audio sounds and usually provides ports in the back of a computer for external speakers. It is installed in one of the expansion slot inside the system unit's motherboard.

A sound card enables computers to out-put quality sounds and music User commonly purchase soundboards to hear the sounds of a game or to play some from a multimedia CD. Some sound cards are capable of recording sounds, music and voice messages.

Although sound cards differ, most provide an output line for speakers, input lines for mono or stereo recording and a MIDI (Musical Instrument Digital Interface) interface for electronic instruments.

MIDI is a standard that allows you to connect your computer to a wide

4. The Modem

The modem is a device that allows a computer to communicate with another computer through a telephone line. Both computers need compatible modem. With a modem, a computer and required software, you can connect with other computers all over the world.

How to Use Modems

a. Modems are used for file transfers that are to copy files and programmes from one computer to another computer. When you copy files from another computer to your computer, you are downloading, and when you are copying files from your computer to another computer you are uploading.

b. Modems are used for fax services. The fax modem enables you to use your computer to send and receive faxes through a fax machine or another computer that is equipped with a fax modem. To send and receive faxes you need fax software.

c. Modems are used for online services.

Modem Speed

Modems are available in different speeds which determine how long it takes to transfer information. The speed of modem is commonly rated in bits per seconds' bps. The higher the bps, the faster data can be transmitted between computers. Naturally faster modems are more expensive. The range of speed of modem includes 2400 bps, 9600 bps, 14,400 bps (14.4 kbps) 33,600 bps (33.6 kbps) 56,000 bps (56kps).The most common and recent are the 33.6 kbps and 56 kbps.

4.0 CONCLUSION

The basic components of the computer system have always remained the same. But with time and advancement in technology the capabilities and capacity of the components have continued to change. One has to be abreast of facts to follow the trend in computer components.

5.0 SUMMARY

- A personal computer is not a single unit. A typical computer consists of several basic parts or components that work together.

- Input devices are the computer hardware that accepts data and instructions from a user. Input devices have been built in many forms to help in communicating with the computer.

- Basically two components handle processing in a computer: the central processing unit (CPU) and the memory.

- Among the most important part of a computer system are the devices that allow you to save the product of your labour. The physical components or materials on which data are stored are called storage media.

- Output devices return processed data, that is, information back to the user. In other words, output devices allow the computer "talk" to us. The most common output devices are the monitor and the printer. Others include modems and speakers.

- The printer is an output device that produces on hard copy or a print out on a paper i.e. it takes data from its electronic form and prints it out on paper.

- Sound cards, otherwise known as soundboards, are hardware boards. They are devices that produce audio sounds and usually provide ports in the back of a computer for external speakers.

- Modems are used for file transfers that are to copy files and programmes from one computer to another computer.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss the types of mouse commonly available.
2. What are the criteria used to select printers in organizations.

7.0 REFERENCES/FURTHER READINGS

Anderson, R.G (1994). Data Processing: Principles & Practice, Vol. 1. Pitman Publishing.

Anderson, R.G, (1994). Data Processing: Information Systems & *Technology, Vol. 2. Pitman Publishing.*

French, C.S. (1993). Computer Studies. DP Publishing Ltd.

Norton, P (1995). Introduction to Computers. Macmillan/McGraw-Hill.

Ron, W (1995). How Computer Works. Macmillan Computer Publishing.

MODULE 2

UNIT 1 COMPUTER COMMUNICATION NETWORKS

CONTENTS

1.0 INTRODUCTION

A computer network is a collection of hardware and software that enables a group of computers to communicate. A network is formed when one or more computers are linked together and are aware of one another and can pool their resources.

The need to communicate and share information with others gave rise to personal computer (PC) network. With a network you can retain the benefits of the personal computer (your own selections of software and a place for personal data not for sharing) and regain the benefits of central computing. PC networking is one of the breakthroughs in information technology industry resulting in a major growth area in PC market.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- explain what a network is
- state the objectives underlying basic networks
- use the basic network terms to communicate in discussing networks
- explain the benefits of applying networks in business and corporate organizations
- identify and distinguish the types of networks that are available
- explain network topologies and how they differ one from another.

3.0 MAIN CONTENT

3.1 Network Objectives

The basic objectives of establishing a network are:

- Connectivity: to permit various hardware and software products to be connected and communicate with each other in a seamless way.
- Simplicity: to permit easy installation and operation of all network components.
- Modularity: to enable building of wide variety of network devices from a relatively small set of mass-produced building blocks.
- Reliability: to permit error free transmission of by providing appropriate error detection and correction capabilities.
- Flexibility: to permit the network to evolve as new need arises or new technologies become available.
- Diversity: to diversify network services that can be easily used yet isolate users from the technical details of network structure and implementation.

3.2 Basic Components and Terms

Nodes or Stations are computers and other devices that communicate with each other in a computer network are called nodes or stations. Nodes can be mainframe computers, mini computers or personal computers or they can be devices such as data-entry terminals.

Network traffic is the data that is sent through the network. Network architecture determines how network components work together.

Network software is commonly called the network operating system (NOS). It organizes and controls the computers attached to the network.

Network adapters (or network interface cards) are expansion cards that transfer information to and from the network. Like other expansion cards network adapters are installed inside the system unit.

Cabling or other medium through which network nodes can communicate: A cable connector extends out of the back of the PC and connects to the network cabling.

3.3 Communication Media

Communication/Network media refer to the wires, cables and other means by which data is transferred from source to its destination. The most common media for data communication are twisted-pair wire, coaxial cable, fibre-optic cable, and wireless link.

Twisted-Pair Wire

The twisted-pair wire consists of two copper strands individually shrouded in plastic, then twisted around each other and bound together in another layer of plastic insulation. Except for the plastic coating, nothing shields this type of wire from outside interference, so it is also called unshielded twisted-pair (UTP) wire.

Twisted-pair wire is commonly known as telephone wire. Because it was readily available and inexpensive, telephone wire gained favour as a conduit for data communications. Twisted- pair wire grew out of that technology but it is now made to more specifications, that is voice-grade telephone wire. All it takes to connect a telephone to a wall plug is a flat pair of wires, but twisting the wires provides a stronger and higher-quality signal. Some networks actually use common telephone wires, but the higher-grade wire is recommended.

Coaxial Cable

Coaxial cable, sometimes called coax is widely used for cable TV and supplanted twisted-pair wire for a while as the medium of choice for networks. There are two conductors in coaxial cable. One is a single wire in the centre of the cable; the other is a shield that surrounds the first wire with an insulator in between. Although it does not have any more conductors than twisted-pair, coaxial cable, because of the shielding, can carry more data than older types of twisted-pair wiring.

Two types of coaxial cable are used with networks: thick and thin. Thick coax is the older standard and is seldom installed in new networks. Thin coax can carry just as much data as thick coax, but it is smaller, lighter, and easier to bend around corners. Today's coaxial cables can carry data at up to about 10Mbits per second, which is relatively slow compared to the 100-Mbit capacity of fibre-optic cable and twisted-pair wiring.

Fibre-Optic Cable

A fibre-optic cable is a thin strand of wire that transmits pulsating beams of light, instead of electrical frequencies. When one end of the strand is exposed to light, the strand carries light all the way to the other end- bending around corners with only a minute loss of energy along the way.

Because light travels faster than electricity, fibre-optic cable can easily carry 100-Mbits per second. Although the twisted-pair wire attain data-transfer rate this high, fibre-optic cable is immune to electromagnetic interference that is problem for copper wires.

One of the problems with fibre optic is the physical routing of the cable. Because the carrier itself is a strand of glass, it does not turn corners easily. A thin strand of glass is more flexible than you might think, but is not nearly as flexible as copper wire.

The most impressive advantage of fibre-optic is its capacity. Because it transmits light instead of electricity, the fibre-optic cable is also immune to many kinds of interference that can cause errors in other media, especially in twisted-pair wire.

Although it is efficient, fast and precise, fibre-optics cable was until recently very expensive. As costs have come down, it has become increasingly popular, and is now revolutionizing a number of communications industries. Telephone and cable-television companies are moving from twisted-pair wire and coaxial cables.

Wireless Links

As data communications have become more common, there's been a push toward more flexible media, and towards media that can span greater distances. Various types of wireless media links provide these advantages.

When portable computers are networked, radio waves can be used as a communication media. For example, companies that specialize in taking inventories for large businesses or supermarket can count all the items in stock using small portable computers that send and receive radio signals. As people move around the store, their computers continually send information back to a central computer that is brought to the store for the purpose.

Permanent networks with wireless links are also becoming important, especially in situations where it is difficult to run physical wires.

Radio frequencies can also be used on a wider geographical scale. Cellular phones, for instance, transmit using radio frequencies. Microwaves that are a type of radio wave are often used when data need to be sent several miles. Microwave communication links do require an unobstructed line between the two antennae.

When communication links cover thousands of miles, communications satellite may come into play. When you call across the country or around the world on a telephone, your voice travels over cables only as far as the nearest satellite-transmission station. From there the signal is beamed to a satellite, which sends it to another transmission station near the destination of your call. Telephone companies are not the only ones

that use satellites, many large businesses and universities also use satellites for data communications.

3.4 Uses of Network

In business, government, schools and other types of organizations, networks of all types of computers provide tremendous benefits. These benefits among others include:

1. Share Information: Networks allow users to share information easily. For example the electronic mail system enables co-workers to send memos to each other. This accelerates the distribution of company information. Users can send written messages without worrying about whether the user is using the computer or not. E-mail has provided businesses with an entirely new and immensely valuable and fast means of communication.

2. Shared Resources: Resources shared under network are:

Application Programs: It is a fact that in business computing most workers uses the same programs. With a network, businesses can save a lot of money by purchasing special network versions of the most commonly use program rather than buying separate copies for each machine. When employers need to use a program, they simply load it from a shared storage device into their own PC. Since a single network copy of the program can serve the needs of a large number of users simultaneously, the entire program would occupy a local hard drive/disk.

Share Data File: The same is true of data that multiple employees need access to at the same; time for example daily stock trade figures in a stock trading firm. Here the issue is data integrity, rather than money. If employees keep separate copies of data on different hard disks, updating the data is very difficult. As soon as a change is made to the data on one machine, there is a discrepancy and it becomes very difficult to know which data are correct. Keeping data that is used by more than one person on shared storage devices solves the whole problem.

Share Peripheral Device/Hardware: Networks enable everyone in an office to utilize the maximum amount of available equipment. For example, by sharing one printer among several computers, cost is reduced. If you have different computers in a work setting, networking enables more people to capitalize on each computer's strength.

Easy Back Up: In business for example financial institutions, data can be very extremely valuable, so making sure that employees back up their

data is one way to address this problem. Employees gain access through a network. That way, one person can be charged with making regular backups of the data on the shared storage device.

3.5 Types of Network

Computer networks can be designed in different ways depending on their:

1. Physical environment (office, factory, college campus) or
2. On the way they are used or organized; for example connecting a few computers to a printer and file server, or connecting thousands of automated teller machines to a distant bank computer.

Types Based on Physical Environment: In describing network using physical environment, two categories are recognized and these are Local Area Network (LAN) and Wide Area Network (WAN).

a. Local Area Network (LAN)

Local area network (LAN) is a network of computers of any variety that are located relatively near each other and connected by a contiguous wire/or a wireless link.

A LAN can consist of just two or three computers connected together to a shared resource, or it may include several hundred; for example a LAN might serve a bank branch consisting of cashiers, clerks, supervisors an accountant and a manager offering banking service to its customers. The LAN can allow these users to exchange messages and documents and to print files and client accounts on shared network printer.

WIRELESS LAN: Wireless LAN is good for:

- Difficult wiring environments such as historic buildings and where cabling can be expensive.
- Frequently changing environment such as banks and stores where the rearrangement of works locations needs to be done quickly without additional costs.
- Temporary LAN for special projects or peak times such as in banks and retail outlets (during peak periods) and exhibitions.
- Metropolitan Area |Network (MAN) for a distance of up to 15km and even more.

b. Wide Area Networks (WAN)

A wide area network (WAN) is typically two or more LAN that is connected together, generally across a wide geographical are. The connections are made by telephone, satellite, fiber-optic backbones or other long distance connections.

For example, a wide area network might be used by a financial institution's central computer system connected to many branches nationally. Such a system continuously receives records of customer transactions from remote sites and updates customer's files accordingly.

The connections in a WAN are often made over equipment that is not owned by the user's organization.

A telephone company or other sellers of telecommunications equipment might provide the WAN services.

Comparisons between Local Area Network and Wide Area Network

	Criteria	Local Area Network	Wide Area Network
1	Media (Link)	Cables	Telephone
2	Number of computers	2 or a hundred	Numerous
3	Ownership of link	User	Another company
4	Location of computer	Relatively close	Distant
5	**Transmission**	**High**	Moderate

Types Based on Network Usage: In describing networks based on how a network is used, i.e how network computers interact and are organized, two categories are identified: client server relationship and peer-to-peer.

c. Client – Server Network

Client-server networks are built around specialized computers called servers that run a network operating system (NOS). Servers perform services on behalf of other network devices, they contain information or computing resources that are shared in other words, clients-server networks is a hierarchical strategy in need- and sometimes the processing needs of all network node (clients).

Once the servers are set up, the clients running under normal PC operating system access information stored either on the server or resources attached to the server. These resources are disk space, shared files, printers, modems, or other specialized hardware. In a client server network, the entire computer shares the resources of the server.

d. Peer-to-Peer Network

Peer –to-peer network is a strategy in which computers on the network can act as both a client and a server. In other words, each node (client) has access to all or some of the resources on other nodes. All the computers run a network operating system (NOS) rather than a PC operating System.

Peer-to-peer networks are flexible. Users can share any part of their systems with other users on the network. However, peer-to-peer networks can be difficult to manage and control because the resources are spread out and not central to one server.

Peer-to-peer network allows users to share peripheral devices including disk storage, so that they have access to data and data and programmes. In addition, some very high-end peer-to-peer networks such as networks of UNIX Computers allows distributed computing which enables users to draw on the processing power of other computers in the network, peer-to-peer networks not only enhances each user's power and productivity, but has the added benefit that no Central host system can fail and suddenly disable all users.

Comparisons between Client-Server and Peer-To-Peer Network

Client-Server	Peer-to-Peer
Server runs a NOS	No server
Clients run PC operating system	The PCs run NOS
All PCs do not perform same functions	All PCs perform same functions

Dependent	Independent
Easy to manage and control	Difficult to manage and control
Centralized resource	Decentralized resource
Rigid	PCs acts both as client and server
Network can easily be disabled	Flexible
	Enhances users power and productivity
	Network cannot be easily disabled

Value Added Networks (VANs)

Value Added Networks (VANs) are public data networks that add value by transmitting data and by providing access to commercial databases and software. VANs are complex technical systems that have traditionally used packet switching, as they can be accessible from different types of workstations.

The use of VAN is usually by subscription, with the user paying for the amount of data they move. As a way to transmit computerized data, they offer a service similar to what the telephone networks do for telephone calls. They are often used in the electronic data interchange (EDI) system because they reduce the complexity of connecting to the disparate EDI of various trading partners. In this application they collect forms in an electronic mailbox, translate and forward them to recipients and guarantee they will reach the destination intact. Other common VAN services include electronic mail, access to stock market data and other public databases, and access to electronic banking and other transaction processing services.

VANs are used for a number of reasons:

They are cost-effective solution for companies that need data communication services but don't want to invest in setting up their own service networks. They are commonly used by companies that lack the technical expertise to maintain a network.

Even small companies can enjoy the benefits of data communications by using VANs and leaving the technical details to the vendors. VANs permit companies to use part of the network instead of paying a large fixed cost for their own underutilized network.

VANs also provide for easier expansion because they are set up use their capacity efficiently and to bring in new capacity if necessary.

Finally, VANs can provide convenient access to data that would not otherwise be available.

The widespread acceptance of Internet is creating an alternative to VANs for many applications that do not involve huge amounts of data.

3.6 Network Topologies

Network topology is the physical layout of the wires that connect the node of the network. In other words, it is part of network architecture that prescribes how you may arrange network devices relative to one another.

Factors Influencing Choice of Topology

There are a number of factors to consider in determining which topology is the best for a given situation. Among the considerations are the type of computers currently installed, the type of wiring now in place (if any) the cost of components and services required to implement the network, and the desired performance.

Types of Topology

There are three common topologies: Linear Bus, Star and Ring topologies

1. Linear Bus Topology

A linear bus topology like the bus of a computer itself is a single conduit/cable to which all the network devices (nodes) and peripheral devices are attached.

A bus network always has two distinct ends rather than a continuous loop of cables. Transmissions on a bus are broadcast along the entire length of the cable. The receiving device (node) whose address matches the destination address of any packet accepts and reads the packet, while the others simply ignore it. On the other hand, nodes on a bus network transmit data and hope that the data will not collide with data transmitted by other nodes, if they do; each node waits a small random amount of time, then attempts to retransmit the data.

The linear bus topology is highly effective and reliable because no central controlling devices are required so no central failure can bring down the network. On the other hand, linear typology is a disadvantage because of the likely collision of data signals sent by nodes. Collision

avoidance and correction require extra circuitry and software to implement and a broken connection can bring down the whole network.

2. Star Topology

Star network is located out so that all of its nodes radiate from a central controlling node. The controller can be a computer running special software or a dedicated routing device called a switch. The controlling node is connected to each network node through a dedicated channel, so it can explicitly direct a transmission to any one node rather broadcast if to the entire network. This scheme has an advantage in that the hub monitors traffic and prevents collisions and a broken connection will not affect the rest of the network. However, if you loose the hub, the network goes down.

3. Ring Topology

In a ring network topology, all network devices are connected in a circular chain forming a closed loop. The final node in the chain connects to the first to complete the ring. With this methodology, each node examines data that are sent through the ring. If the data is not addressed to the node examining them, that node passes them along to the next node in the ring.

The ring topology has a substantial advantage in that there is no danger of collisions because data always flow in one direction. The disadvantage to the ring topology is that if a connection is broken, the entire network goes down.

4. Hybrid Topology

The linear bus, star ring are sometimes combined to form combination or hybrid networks. A hybrid network in a high – rise building might use linear bus to run up and down the height of the building, and ring or other topologies on each floor.

3.7 Network Protocols

Network protocols are a set of standards for network communication. In other words, they are like the language for communicating data for computers. Note that for computers to communicate they must speak the same language.

Types of Network Protocols

1. Ethernet: It is currently the single most common network protocol.

Ethernet uses the linear – bus topology and is inexpensive and relatively simple. With a linear-bus, however, each workstation must take its turn to send data, and when there are many computers on an Ethernet network; access time can become noticeably delayed.

One of the newest standards in networks implements Ethernet using the 10base-T. This standard uses equipment that provides the convenience of a centralized star topology with the flexibility and a linear-bus. The Ethernet network buses are limited to 2500 feet in length and run at 10 Mbits per second.

2. Token Ring: As the name implies it is based on token ring topology. Controlling hardware transmits the electronic address of each workstation on the network many times per second. Each workstation examines these addresses to see whether one is its own.

Token ring network has the advantage of data travelling in a controlled manner through the ring in one direction. Token ring is expensive and operates at 4 or 16 Mbits per second or even more.

3. Arcnet: This protocol is based on star topology. The star is perpetuated by hubs attached to the network. Arcnet is very slow; about 2.5 Mbits per second, but it is inexpensive, reliable and easy to set up and expand. Faster versions of Arcnet are forthcoming.

4.0 CONCLUSION

The concept of networking is revolutionary in the computer industry, bringing about sweeping changes in telecommunications. Globalization of business, commerce and governance has been made possible because it is now possible to link computers together over wide geographical area. Imagine a world of Internet without networking concepts.

Though there were difficulties in perfecting the act of networking, advances in technology has made it possible to easily deploy networks. It is worthy for you to know that networking is the platform on which ICT is driven.

5.0 SUMMARY

You should consider these salient points as a summary of this unit:

- A computer network is a collection of hardware and software that enables a group of computer to communicate. A network is formed when one or more computers are linked together and aware of one another and can pool their resources.

- The basic objectives of establishing a network include connectivity, that is, to permit various hardware and software products to be connected and communicate with each other in a seamless way.

- Computers and other devices that communicate with each other in a computer network are called nodes or stations.

- Communication/Network media refer to the wires, cables and other means by which data is transferred from source to its destination. The most common media for data communication are twisted-pair wire, coaxial cable, fibre-optic cable, and wireless link.

- Local area networks (LAN) is a network of computers of any variety that are located relatively near each other and connected by a contiguous wire/or a wireless link.

- A wide area network (WAN) is typically two or more LAN that are connected together, generally across a wide geographical are. The connections are made by telephone, satellite, fiber-optic backbones or other long distance connections.

- Client-server networks are built around specialized computers called servers that run a network operating system (NOS).

- Peer –to-peer network is a strategy in which computers on the network can act as both a client and a server.

- Value Added Networks (VANs) are public data networks that add value by transmitting data and by providing access to commercial databases and software.
- Network topology is the physical layout of the wires that connects the node of the network. In other words, it is part of architecture that prescribes how you may arrange network devices relative to one another.

7.0 REFERENCES/FURTHER READINGS

Anderson, R.G (1994). Data Processing: Principles & Practice, Vol. 1. Pitman Publishing.

Anderson, R.G, (1994). Data Processing: Information Systems & *Technology, Vol. 2. Pitman Publishing.*

French, C.S. (1993). Computer Studies. DP Publishing Ltd.

Norton, P (1995). Introduction to Computers. Macmillan/McGraw-Hill.

Ron, W (1995). How Computer Works. Macmillan Computer Publishing.

UNIT 2 THE INTERNET

CONTENTS

1.0 INTRODUCTION

What is the Internet?

The Internet commonly referred to as the 'Net' is better described than defined, as a global network of computers. It is often described as a network of networks because it first began through the linking of the existing local computer networks used by universities and governmental organizations. The Internet is a constellation of computers around the world that speak the same language so information travels seamlessly from one computer to another. Globally, the Internet connects scientific research, educational, government, commercial and business networks. When you connect to the Internet, your computer becomes part of the global network of computers. The Internet is more than a technological marvel. The peace is quick, with messages and information racing round the world in a few seconds. It has ushered in an era of sweeping changes in networking and communication that has left no business, agency, organization or government untouched.

Various estimates all over the world placed the global online population (i.e. people accessing Internet connections and accounts) at a little over 600 million in late 20002 (Nau.com 30 January, 2003; UNCTAD 2002). In Nigeria, about 200,000 (as at 1999) were using the Internet and this number was projected to have hit 18 million by 2003 (Nigerian Government).

By the year 2002, $400 billion worth of business transactions were passing over the Internet worldwide. As at 1998, 10 million Europeans banked on the Internet and by 2003 there were $100 million online bank accounts in the USA. The big attraction for business is that the Internet offers real –time information and interaction and allows even the smallest firms to reach a global audience.

What is Intranet?

An intranet is a local area network that companies use to distribute information and speed up the movement of data within offices. In other words an intranet allows the job of processing to be distributed among multiple computers. Intranet activities usually take place behind secure 'firewalls' that only authorized users have access to. An intranet can span multiple business locations via the Internet. Intranets are built using the same standard Internet software such as TCP/IP, e-mail client, web browser and telephone dialer.

What is Extranet?

When a company throws open its internal network or intranet to selected business partners, the intranet becomes an extranet. Suppliers, distributors and other authorized users can then connect to the

company's network over the 'Net' or through virtual private networks. Once inside, they can view the data the company makes available.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- explain what the Internet is and distinguish it from related terms like intranet and extranet
- trace the origin of the Internet to give you a better understanding of the trend in its development
- recount the benefits of the Internet to business, commerce, governance and education among others
- state the necessary infrastructures for connecting to the Internet
- recount, for business purposes, the various services offered on the Internet
- explain the application of the Internet in business through case study.

3.0 MAIN CONTENT

3.1 How the Internet Developed

The Internet began in the 1960s when the US Department of Defense through ARPANET (Advanced Research Project Agency Network) began creating a computer network that would continue to function in the event of a major disaster. In 1969, four mainframe computers at a U.S. university were linked into a network that transferred data on dedicated high-speed transmission lines. Through the 1970s and 1980s new similar networks were created to link educational institutions, government offices and military centers in the United States and other countries. In the 19990s, as the Internet grew, private businesses and other regional network providers took over the operation of the major Internet networks and the development of much of the information available online. Private businesses, educational institutions, organizations and individuals now develop much of the information content available online.

3.2 How Information is transmitted on the Internet

The Internet is a worldwide complex of small regional networks. To understand this, picture a major road connecting large cities. Smaller

roads link the cities to small towns where residents travel on narrow residential streets. The high-speed Internet is the major road in this scenario. Connected to it are smaller computer networks (functioning like smaller, less traveled roads) that can share data information at high speeds. In order to enable different computers to communicate and transmit packaged information with each other, a standard 'protocol' has been established for transporting data. This Internet protocol is called Transmission Control Protocol/Internet Protocol (TCP/IP) and allows all networks all over the world to communicate with each other on the Internet.

When transmitting information over a network or the Internet, it is in the same binary form as when it is stored on a computer, but the data has to be packaged for transmission. This procedure is necessary because bits travelling freely on the network will have no meaning to devices. So before data is transmitted on the Internet, network software forms the data into packets. A packet among others includes:

- The user information that is intended for transmission
- The addresses of the sender and the destination
- Additional information about the type or purpose of the transmission.
  This information tells the network device at the receiving end (and any connecting device along the way) what to do with the packet. Packet formatting allows the Internet network to control where information goes and how it is treated once it arrives there.

A protocol is a code of interaction for a specific situation; so, network protocols are the rules that network devices, over the Internet, follow to successfully interact with one another.

3.3 Benefits of the Internet

Basically and generally, the benefits derivable from the utilization of the Internet are mainly as follows:

Speed/Time Saving: The speed of transmission on the Internet is the significant benefit of the Internet. A letter or document that could take days to arrive by regular mail can be sent to the other side of the world in minutes. Likewise, searching through a card catalogue at a library can be a time consuming, tedious process, but you can search an online version of the same catalogue in a fraction of the time. The speed of transmitting information naturally saves time and money.

Breadth/Reach: The Internet gives you access to a vast (and growing) collection of databases, documents, computer software; these and almost any other kind of information can be stored electronically.

Cost Saving: Exchanging information via the Internet is less expensive than using telephones or fax machines especially where telephone access fees are high. Likewise marketing and advertising your products and services on the Internet can be less expensive than using conventional printing and document-delivery methods.

Two-way Communication: Audiences now have the means to respond directly to sources of information, research and opinion.

Trading: The Internet provides the opportunity for purchase and sale of goods and services.

Specifically, the Internet through the E-Commerce has provided the business community, among others, the following benefits:

i. Improved response time to clients' requests
ii. Improved competitive position
iii. Eased the process of concluding deals and financial transactions
iv. Extended market reach and increased revenue potentials
v. Increased consumer convenience and choice
vi. Reduced prices
vii. Improved customer service.

3.4 Services Offered on the Internet

Many electronic services are available on the Internet. With consistent development of the Internet technology itself and with the infrastructure supporting the services offered on the Net, the Internet continues to grow.

The major Internet services are as follows:

1. Electronic Mail (e-mail)

This is the most popular and most utilized Internet service especially in the developing countries of the world. A conservative estimate puts the number of people using the e-mail worldwide at more than 90 million people.

E-mail is message sent from one person to another via a computer network. The same e-mail can be sent easily to one address or many addresses. Commercial electronic mail is used for the same purposes as the organization wide mail system. But instead of being limited to members of one organization, the service is made available to the public on subscription bases. E-mail messages are exchanged between customers, suppliers, friends and business partners. E-mail service has

cut down on the cost of mailing or sending information thus saving time and money.

E-mail is used as a marketing tool. For example, a company, Dealaday.com uses e-mail to prospect for customers and sends group e-mail to 10,000 user names all customers who have indicated they would like to receive e-mails. With e-mail they receive a 7%, 8% and sometimes 10% response, unlike 1% or 2% response in normal direct marketing.

2. The World Wide Web (WWW)

The World Wide Web or the web is one of the Internet's most popular applications and it was launched in 1991. It is a graphical, easy –to-use way to organize and present information, including texts, images, movies, sounds and more. The World Wide Web has generated tremendous popular interest in the Internet.

The www is unique for two reasons. Firstly it is highly interactive media bringing documents in graphics, audio and video. Secondly, it uses hyperlink, which provides connections between different resources. It allows users to jump from one page to another. A file in www is called the home page and usually contains a multimedia clip. A page can link you to other web pages and Internet resources with clicks of a mouse. You can view and download any information you need on any home page with the aid of software known as the web browser.

The web browser translates a home page address called a URL (Universal Resource Locator) and downloads the home page so that you can see it on the screen. Generally browsers are software used to access and view sites on the World Wide Web. Some of the popular ones are Netscape, Navigator and Microsoft Internet Explorer. Netscape offers info seek and Lycos. Others are yahoo, and WebCrawler. The basic language of the www is hypertext markup language [HTML] that is used to determine what the information will look like and point to where you can find the links.

The web is based on a protocol called hypertext transport protocol (http) and covers the entire operation of the web. The http runs on top of the TCP/IP (the usual Internet protocol). As information on the web gets easier to find, it is becoming more useful as a tool for everyday business.

As a commercial service, the web is basically used to advertise and sell goods and services, streamline operations and automate customer services. With the help of the web, businesses are wringing out time out

of product design speeding up the order and delivery of components, tracking sales by the hour, and getting instant feedback from customers.

The main drawback to the use of the www is that it consumes a lot of space thereby slowing the download time. For example 5 minutes of audio can take 5 megabytes of memory. Therefore the www uses up a lot of hard drive space.

3. File Transfer Protocol (ftp)

File transfer protocol (ftp) is an Internet tool used to transfer files between computers and it is the most common method of transferring files on the Internet. Without viewing them as they are transferred the ftp enables you to access file on a remote location on the Internet once you log on to an ftp site, and you are able to access all files on sites and download them if you so desire. It is fairly easy to publish information on the Internet. Many institutions maintain publicly accessible archives of information that they want to share with others.

4. Newsgroups

Newsgroup is an Internet service whereby people with common interests share information or seek advice over the Internet. Newsgroups do not operate as e-mail, sent directly to e-mail addresses, but as feed that is sent to specific servers around the world. This feed happens at specific times of the day, not when there is a new message posted to the newsgroup. The institution operating the computer system that provides you with the access to the Internet (Internet Service Provider or a university) selects the newsgroups it wishes to subscribe to, and this is the only newsgroup you will be able to get.

5. Telnet

Telnet is an Internet service that allows you to connect to a remote computer to use specific databases or other applications available on that computer.

Telnet is one of the first applications widely used on the Internet. Many telnet applications are now available on the World Wide Web where they are easier to use.

6. Internet Conference

This is an Internet service whereby different techniques are used to allow people to discuss topics of mutual interest. A conference can be as simple as sending e-mail to many different people or as complex as

arranging to have people link different cities, see images of each other and hear each other talk in real time- that is video conferencing. Internet conferencing is possible, but the technology becomes more complex and the speed of the connection becomes more important as you go from text only, to transmitting sound and video in real time. Internet conference brings about tremendous savings on travelling, time and money.

7. Internet Telephony

This is a service in which you can use the Internet as a voice telephone line. With some types, both you and the person you are calling must have an Internet connection and be online at the time you wish to talk. Some companies also offer Internet-to- telephone services where from your computer you can call any telephone number in the world.

Internet telephone services are inexpensive when you compare with the conventional cost of telephone services. If your organization spends a lot of money on long distance telephone calls, this might be a good option for you. There are growing numbers of companies providing Internet telephone services.

8. Internet Fax

Internet fax is a service that takes a special type of e-mail message and sends it to a fax machine specified in the message. The message can be faxed to a computer (Internet-to-Internet).

9. Listserv

Listserv is an Internet application that allows subscribers to send an e-mail that will be received by all people who subscribe to the Listserv. Subscribing to the list and all other transactions are handled through e-mail. Listservs are a powerful and inexpensive way for people with shared interests to communicate quickly and cheaply with an entire group of people. Sending an announcement to a listserve is like immediately publishing or broadcasting your remarks. Many organizations are happy to host listservs that conform to their interests. Because of the different types of software, you will often hear listservs called by other names such as listproc or majordomo

10. Gopher

The gopher is an Internet service of making text- only material available over the Internet so it can be viewed online. Gopher servers were widely used before the advent of the world wide web, and there are still many in operation. They can be accessed through the web browser.

11. Internet Relay Chat (IRC)

This is the multi-user chat system where people convene on channels (Virtual Place usually with a topic of conversation) to talk in groups, or privately. In other words IRC allows you to talk to other IRC users worldwide in real time via your keyboard.

3.5 How to Connect to the Internet

To be connected to the Internet and partake of the numerous services offered on it, the basic requirements are as follows:

1. A computer
2. A telephone line
3. A modem
4. An Internet service provider
5. A communication software

Theoretically, a personal computer of any age can be connected to the Internet as long as you can plug it into a modern. For effectiveness and a more practical utilization of the Internet facilities you need nothing less than a 386, although the choice of PC is dependent on the type of Internet service needed. For example a 386 or 486 PC is good enough for personal e-mail services, newsgroup or Listserv, These services do not require graphics. However, you need a Pentium PC for such services as the World Wide Web and Internet conference.

The Telephone

The telephone line could be either analog or digital like is preferable for efficiency. Depending on need, a line can be dedicated fully for Internet services only.

The Modem

A modem allows one PC to dial in to another PC. A modem is a device that allows one computer to communicate with another through a telephone line.

Modems are of different speed/capabilities ranging from 9600bps to 56 kbps. When you are using the Internet the speed at which things work is

more likely to be limited by the speed of your modem than by that of your computer. The faster the speed of transmission by a modem, the better for the Internet user.

3.6 The Internet Service Provider (ISP)

For a modem to bring you information it, has a number to dial. This is where an Internet service provider (ISP) comes in. The ISP is the organization that gives a subscriber access to the information superhighway. So to be connected to the Internet you need to subscribe to an ISP.

There are several ISPs scattered all over the world; some of the popular ones are American Online (AOL), UK Line and CompuServe.. Here in Nigeria, some of the common ones are Hyperia, Infoweb, Cyberspace, Linkserve, Nigeria Online, Nigeria Net, Nitel, Nova, Prodigy, etc

The choice of an ISP depends mostly on the effectiveness in the transmission of information, that is, speed of service is an important criterion for selecting an ISP. The efficiency of an ISP, in terms of speed of transmission of information, can be determined by the bandwidth it can support. A bandwidth is a measure of the amount of data satellite link etc. The bandwidth available determines the total capacity of an ISP to move data anywhere in the world.

3.7 Case Study: Interactions between Internet, Intranet and Extranet: The Case of Cool Sportz Corp

Cool Sportz sits at the centre of a web of partners all connected over the Internet using open software standards. It has a private intranet to communicate with branch stores and employees in remote offices. A secure extranet links Cool Spotz to its contract manufacturers, suppliers, independent retailers, distributors, and partners, such as law firms and ad agencies.

The Use of the Intranet

Cool Spotz uses its intranet for the following areas:

- Retail Store: Cool Sportz collects all sales data from its 1200 retail stores around the country and fills hundreds of product selections electronically. All stores are on the Cool Sportz Intranet, a secure line that transverses the Internet. Cool Spotz also ‘pushes’ info on promotions and discount to its stores.

• Employees: Instead of phoning the HRD, Cool Sportz staff refer to an electronic version of the employee commissions and read up on new merchandise marketing programmes.

• Partnership: To help efficiency, Cool Spotz requires its law firm, accounting firm and ad agency to belong to the corporate extranet. This ensures privacy and security for e-mail and electronic files. Cool Spotz marketers brainstorm over the extranet with the ad agency.

• Office Supply: To centralize the purchasing of office supplies, Cool Spotz lets managers in retail stores have requisition from diskettes to display racks through their PCs. The orders are sent over the extranet from Cool Spotz to suppliers, who deliver directly to the stores.

• Product Design: Cool Spotz enlists reliance designers to create CoolWear products. The designers exchange draws with Cool Spotz over the extranet. Then Cool Spotz's staff and designers can make them up while talking together live over the Net.

The Use of the Internet

• Purchasing Cool Spotz used to order shoes, ski gear and camping goods by phone and fax. Now Cool Spotz saves time and money by sending orders electronically over the Internet. Some suppliers allow Cool Spotz to enter their private network to place orders.

• Consumers: Cool Spotz's web site is promoted in TV ads and gets thousands of hits a day. From surveys on its site, Cool Spotz collects demographic data, and it advises registered surfers on sales and new products.

• Liquidation: When products don't sell, Cool Spotz auctions them through an online brokerage. The company posts information about the goods and a minimum price. Potential buyers enter bid and Cool Spotz ships the goods to the winning bidder.

Manufacturing: For years, Cool Spotz has placed orders with contract manufacturers using Electronic Data Exchange or EDI an old software standard that is neither cheap nor flexible. Now, Cool Spotz saves money by moving some of these orders over the Internet.

4.0 CONCLUSION

The Internet has indeed turned the world into a global village, where businesses, both local and international, are reduced to clicks of the

button. Despite the negative side to the use of the Internet, its advantages far out way the disadvantages. It has got to the point where businesses cannot do without the Internet.

The seeming challenge of the Internet is the issue of bandwidth, especially within developing economies of the world. It is heart warming to know that efforts are geared towards improving the state of bandwidth and connectivity as it relates to the Internet.

5.0 SUMMARY

In summary the following are the key issues arising from this unit:

- The Internet commonly referred to as the 'Net' is better described than defined as a global network of computers.

- An intranet is a Local Area Network that companies use to distribute information and speed up the movement of data within offices.

- The Internet began in the 1960s when the US Department of defense through ARPANET (Advanced Research Project Agency Network) began creating a computer network that would continue to function in the event of a major disaster.

- When transmitting information over a network or the Internet, it is in the same binary form as when it is stored on a computer, but the data has to be packaged for transmission.

- The speed of transmission on the Internet is a significant benefit of the Internet. A letter or document that could take days to arrive by regular mails can be sent to the other side of the world in minutes.

- Exchanging information via the Internet is less expensive than using telephones or fax machines especially where telephone access fees are high.

- The World Wide Web or the web is one of the Internet's most popular applications and it was launched in 1991. It is a graphical, easy –to-use way to organize and present information, including texts, images, movies sounds and more.

- Telnet is an Internet service that allows you to connect to a remote computer to use specific databases or other applications available on that computer.

- Theoretically, a personal computer of any age can be connected to the Internet as long as you can plug it into a modern.

- The choice of an ISP depends mostly on the effectiveness in the transmission of information, that is, speed of service is an important criterion for selecting an ISP.

6.0 TUTOR-MARKED ASSIGNMENT

1. Differentiate between the Internet, Intranet and Extranet
2. Mention 5 benefits associated with the use of the Internet in business.

7.0 REFERENCES/FURTHER READINGS

Anderson, R.G (1994).Data Processing: Principles & Practice, Vol. 1. Pitman Publishing.

Anderson, R.G (1994). Data Processing: Information Systems & *Technology, Vol. 2. Pitman Publishing.*

Close, Humphrey & Ruttenbure, (2000). What is Electronic Learning?

Kocher, J. (1995). Internet Passport: Northwest Net's Guide to our *World Online. Bellevue, WA: Northwest Net and Northwest* Academic Computing Consortium, Inc.

Hughes, K. (1994). Entering the World-Wide Web: A Guide to *Cyberspace. Enterprise Integration Technologies.*

The Leland Initiatives (1998). Making the Internet Connection Count: *Effective Use of the Internet in Seven Steps. The Leland Initiative* Team.

Nua.com 2003.

NCTAD, (2002). What is Electronic Learning?

UNIT 3 GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

CONTENTS

1.0 INTRODUCTION

The Global System for Mobile Communication otherwise popularly known as GSM was designed in Europe and its first commercial network was launched in 1991.

During the early 1980s, analog cellular telephone systems were experiencing rapid growth in Europe, particularly in Scandinavia, the United Kingdom, France and Germany. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operations within national boundaries, which in a unified Europe were increasingly unimportant, but there was also a very limited market for each type of equipment, so economies of scale and the subsequent savings could not be realized.

The Europeans realized this early on, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system.

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications were published in 1990. Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries (1). Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers worldwide (2), which had grown to more than 55 million by October 1997. With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile Communications.

The developers of GSM chose an unproven (at the time) digital system, as opposed to the then-standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. The over 8000 pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee proper inter working between the components of the system. This is done by providing functional and interface descriptions for each of the functional entities defined in the system.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- identify the origin and trend of the Global Mobile Communication System (GSM)

• state the major services provided by the GSM
• describe the basic architecture of the GSM network
• explain the trend in GSM business in Nigeria
• describe how communication is handled in a GSM network.

3.0 MAIN CONTENT

3.1 Services Provided By GSM

Using the ITU-T definitions, telecommunication services can be divided into bearer services, teleservices, and supplementary services. The most basic teleservice supported by GSM is telephony. As with all other communications, speech is digitally encoded and transmitted through the GSM network as a digital stream. There is also an emergency service, where the nearest emergency service provider is notified by dialing three digits (similar to 911).

A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM network to interwork with POTS.

Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by the use of an appropriate fax adaptor. A unique feature of GSM, not found in older systems, is the Short Message Service (SMS). SMS is a bidirectional service for short alphanumeric (up to 160 bytes) messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cell-broadcast mode, for sending messages such as traffic updates or news updates. Messages can also be stored in the SIM card for later retrieval (3).

Supplementary services are provided on top of teleservices or bearer services. In the current (Phase I) specifications, they include several forms of call forward (such as call forwarding when the subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting and multi-party conversations.

3.2 GSM /Mobile Telephone in Nigeria

Following the adoption of the National Telecommunications Policy in 2000 and the award of three GSM (Global System for Mobile Communications) licenses to private operators in 2001, mobile investment and network rollout increased rapidly in Nigeria. The most dynamic new entrant was Mobile Telephone Networks (MTN) of South Africa, which achieved a 42 per cent market share by March 2005. V-Mobile (the majority-owned by private investors) followed with 24 per cent, Globacom followed (100 per cent held by local shareholders) with a 24 per cent market share, , and then M-Tel (fully owned by state-owned incumbent NITEL) with 10per cent. New mobile subscriptions increased from about 28,250 per month during 2001 to more than 500,000 per month in 2004, raising the number of mobile subscribers from 370,000 in 2001 to about 11 million by March 2005. Mobile penetration rates rose from 0.3 per cent to 8.2 per cent over the same period. Industry reports estimate that foreign investment in the telecommunications sector had reached $3.5 billion by the end of 2004, making it the second biggest recipient of private investment in the country, behind only the oil and gas sector. Mobile telephony represented more than 70 per cent of this investment, at $2.5 billion.

3.3 Architecture of the GSM Network

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure 3 shows the layout of a generic GSM network. The GSM network can be divided into three broad parts. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile Services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and set up of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile Services Switching Center across the A interface.

The Mobile Station

The Mobile Station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to subscribed services irrespective of a specific terminal. By inserting the SIM card into another GSM terminal, the user is able to receive calls at

that terminal, make calls from that terminal, and receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The IMEI and the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

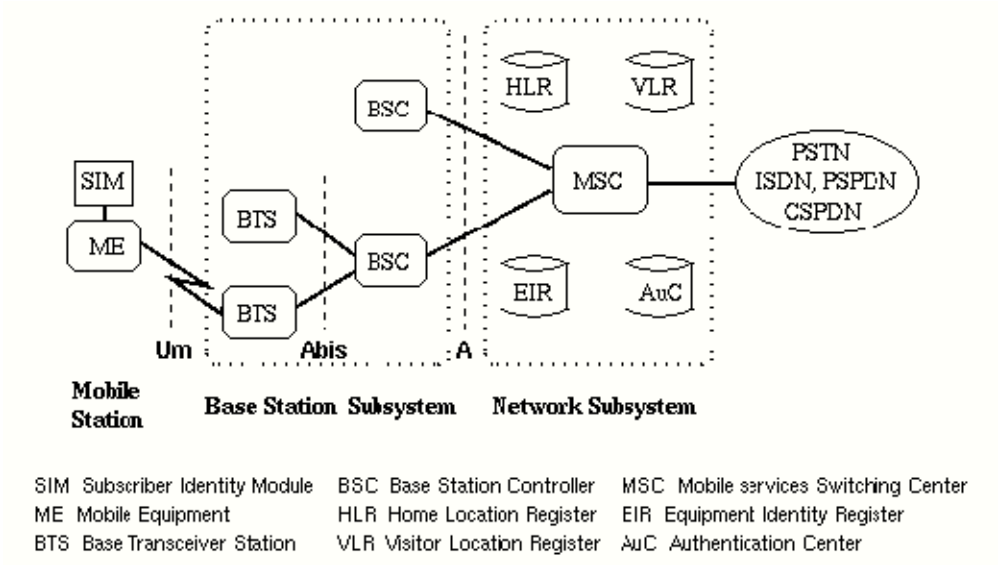


Figure 3 General architecture of a GSM network

The Base Station Subsystem

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the standardized Abis interface, allowing (as in the rest of the system) operations between components made by different suppliers.

The Base Transceiver Station houses the radio transceivers that define a cell and handles the radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed, thus the requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping, and

handovers, as described below. The BSC is the connection between the Mobile Station and the Mobile Service Switching Center (MSC).

The Network Subsystem

The central component of the Network Subsystem is the Mobile Services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the fixed networks (such as the PSTN or ISDN). Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7), used for trunk signaling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signaling required. Note that the MSC contains no information about particular mobile stations --- this information is stored in the location registers.

3.4 Radio Resources Management

The radio resources management (RR) layer oversees the establishment of a link, both radio and fixed, between the mobile station and the MSC. The main functional components involved are the Mobile Station, and the Base Station Subsystem, as well as the MSC. The RR layer is concerned with the management of an RR-session (4), which is the time that a mobile is in dedicated mode, as well as the configuration of radio channels including the allocation of dedicated channels.

An RR-session is always initiated by a Mobile Station through the access procedure, either for an outgoing call, or in response to a paging message. The details of the access and paging procedures, such as when a dedicated channel is actually assigned to the mobile, and the paging sub-channel structure, are handled in the RR layer. In addition, it handles the management of radio features such as power control, discontinuous transmission and reception, and timing advance.

Handover

In a cellular network, the radio and fixed links required are not permanently allocated for the duration of a call. Handover, or handoff as it is called in North America, is the switching of an on-going call to a different channel or cell. The execution and measurements required for handover form one of the basic functions of the RR layer.

Handovers can be initiated by either the mobile or the MSC (as a means of traffic load balancing). During its idle time slots, the mobile scans the Broadcast Control Channel of up to 16 neighboring cells, and forms a list of the six best candidates for possible handover, based on the received signal strength. This information is passed to the BSC and MSC, at least once per second, and is used by the handover algorithm.

3.5 Mobility Management

The Mobility Management layer (MM) is built on top of the RR layer, and handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on mobile station so that incoming call routing can be completed.

Authentication and Security

Since the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be is a very important element of a mobile network. Authentication involves two functional entities, the SIM card in the mobile, and the Authentication Center (AuC). Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the AuC. During authentication, the AuC generates a random number that it sends to the mobile. Both the mobile and the AuC then use the random number, in conjunction with the subscriber's secret key and a ciphering algorithm called A3, to generate a signed response (SRES) that is sent back to the AuC. If the number sent by the mobile is the same as the one calculated by the AuC, the subscriber is authenticated (4).

3.6 Communication Management

The Communication Management layer (CM) is responsible for Call Control (CC), supplementary service management, and short message service management. Each of these may be considered as a separate sub layer within the CM layer. Call control attempts to follow the ISDN procedures specified in Q.931, although routing to a roaming mobile subscriber is obviously unique to GSM. Other functions of the CC sub layer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

Call Routing

Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, a GSM user can roam nationally and even internationally. The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN). This number includes a country code and a National Destination Code which identifies the subscriber's operator.

An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function. The GMSC is basically a switch which is able to interrogate the subscriber's HLR to obtain routing information, and thus contains a table linking MSISDNs to their corresponding HLR. A simplification is to have a GSMC handle one specific PLMN. It should be noted that the GMSC function is distinct from the MSC function, but is usually implemented in an MSC.

4.0 CONCLUSION

Telecommunications are evolving towards personal communication networks, whose objective can be stated as the availability of all communication services anytime, anywhere, to anyone, by a single identity number and a pocket table communication terminal. Having a multitude of incompatible systems throughout the world moves us farther away from this ideal. The economies of scale created by a unified system are enough to justify its implementation, not to mention the convenience to people of carrying just one communication terminal anywhere they go, regardless of national boundaries.

The GSM system, and its sibling systems operating at 1.8 GHz (called DCS1800) and 1.9 GHz (called GSM1900 or PCS1900, and operating in North America), are a first approach at a true personal communication system. The SIM card is a novel approach that implements personal mobility in addition to terminal mobility. Together with international

roaming, and support for a variety of services such as telephony, data transfer, fax, Short Message Service, and supplementary services, GSM comes close to fulfilling the requirements for a personal communication system: close enough that it is being used as a basis for the next generation of mobile communication technology in Europe, the Universal Mobile Telecommunication System (UMTS).

Another point where GSM has shown its commitment to open standards, openness, and interoperability is the compatibility with the Integrated Services Digital Network (ISDN) that is evolving in most industrialized countries and Europe in particular (the so-called Euro-ISDN). GSM is also the first system to make extensive use of the Intelligent Networking concept, in which services like 800 numbers are concentrated and handled from a few centralized service centers, instead of being distributed over every switch in the country. This is the concept behind the use of the various registers such as the HLR. In addition, the signaling between these functional entities uses Signaling System Number 7, an international standard already deployed in many countries and specified as the backbone signaling network for ISDN.

GSM is a very complex standard, but that is probably the price that must be paid to achieve the level of integrated service and quality offered while subject to the rather severe restrictions imposed by the radio environment.

5.0 SUMMARY

- The Global System for Mobile Communication popularly known as GSM was designed in Europe and its first commercial network was launched in 1991.

- Over 200 GSM networks are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers worldwide.

- Following the adoption of the National Telecommunications Policy in 2000 and the award of three GSM (Global System for Mobile Communications) licenses to private operators in 2001, mobile investment and network rollout increased rapidly in Nigeria.

- A GSM network is composed of several functional entities, whose functions and interfaces are specified.

- The Mobile Station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM).

- The central component of the Network Subsystem is the Mobile Services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber.

- The Radio Resources management (RR) layer oversees the establishment of a link, both radio and fixed, between the mobile station and the MSC. The main functional components involved are the Mobile Station, and the Base Station Subsystem, as well as the MSC.

- The Mobility Management layer (MM) is built on top of the RR layer, and handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects.

The Communication Management layer (CM) is responsible for Call Control (CC), supplementary service management, and short message service management.

6.0 TUTOR-MARKED ASSIGNMENT

1. Mention and briefly describe the architecture of a GSM network.
2. Identify and give the functions of the Basic Station Subsystem.

7.0 REFERENCES/FURTHER READINGS

Balston, D. M. (1993). "The Pan-European System: GSM." In Balston, D. M. & Macario, R.C.V. (eds), Cellular Radio Systems. Boston: Artech House.

Déchaux, C. and Scheller, R. (1993). "What are GSM and DCS?" *Electrical Communication, 2nd Quarter 1993.*

Michel, Mouly & Marie-Bernadette, Pautet. (1992). The GSM System *for Mobile Communications. Published by the authors.*

Torbjorn,Nilsson.Toward a New Era in Mobile Communications. http:// 193.78.100.33/ (Ericsson WWW server).

Robert G. Winch (1993).Telecommunication Transmission Systems. New York: McGraw-Hill.

UNIT 4 DATABASE MANAGEMENT SYSTEM (DBMS)

CONTENTS

1.0 INTRODUCTION

A database management system (DBMS) is a computer tool used for the orderly processing, storage and retrieval of data. It is the program or collection of programs that allows users (and other programmes) to access and work with a database anytime. In other words, DBMS is an item of complex system software, which constructs and maintains the database in a controlled way. The DBMS is also defined simply as a computerized record keeping system. The DBMS consists of data, software and the user. It provides the interface/link between the user and the data in the database.

On the other hand, a database is a repository or store for related collection of data. It is also a single organized collection of structured data, stored with a minimum of duplication of data items so as to provide a consistent and controlled pool of data. This data is common to all users but independent of the program which is the data. For example,

an address book (diary) can be a database where the names, addresses and telephone numbers of friends or business contacts are stored. A company database might contain information about customers, vendors, employees, sales and inventory. Each piece of information can be added to a database and extracted later in a meaningful way.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- explain Database Management System
- identify the various types of DBMS programs
- state the basic terms of communications in a DBMS environment
- enumerate the functions of DBMS
- tell who a database administrator is
- explain the role and criteria of being a database administrator.

3.0 MAIN CONTENT

3.1 Evolution of Database Management Systems

Databases have been in use since the earliest days of electronic computing, but the vast majority of these were custom programs written to access custom databases. Unlike modern systems that can be applied to widely different databases and needs, these systems were tightly linked to the databases in order to gain speed at the price of flexibility.

Navigational DBMS: As computers grew in compatibility the trade off in the use of customized database system became increasingly unnecessary; as a number of general-purpose database systems emerged, and by mid-1960s there were a number of such systems in commercial use. Interest in standards started to grow and Charlse Benchman, author of one of such products, IDS, started the database Group Task Group. In 1971 they delivered their standard, which generally became known as **Codasyl approach, and soon there were a number of commercial** products based on it available.

The Codasyl approach was based on the “manual" navigation of a linked dataset which was formed into large network.

IBM also had its own DBMS system in 1968 known as IMS. It was generally similar in concept to Codasyl, but used a strict hierarchy for its model of data navigation instead of Codasyl's network model.

Both concepts later became known as navigational databases due to the way data was accessed.

Relational DBMS: Edgar Codd while working at IBM was unhappy with the navigational model of Codasyl approach, notably the lack of "search" facility which was becoming increasingly useful when the database was stored on a disk instead of on paper. In 1970 he wrote a number of papers outlining a new approach to database construction eventually culminating in the groundbreaking. One of them is titled “A Relational Model of Data for Shared Data Banks”.

In this paper he described a new system for storing and working with large databases. Instead of records being stored in some sort of linked list of free-form records as in Codasyl, his concept was to use a “table” of fixed-length records. Such a system will be inefficient when storing sparse databases where some of the data for any one record could be left empty. The relational model solved this by splitting the data into a series of tables, with optional elements being moved out of the main table where they would take up room only if needed.

For instance, a common use of a database system is to track information about users, their name, login information, and various addresses and phone numbers. In the navigational approach all of this data would be placed in a single record, and items that were not used would simply not be placed in the database. In the relational approach, the data would be split into a user table, an address table and a phone number table (for instance). Only if the address or phone numbers were provided would records be created in these optional tables.

Multidimensional DBMS: The multidimensional DBMS ignores the logical/physical independent tenets of the relational model and instead exposes pointers to the programmer. Due to poor timing and generally poor implementation, as general solution the multidimensional system never became popular, although certain ideas have been picked up in object DBMS.

Object DBMS: Multidimensional DBMS did have one lasting impact on the market; they led directly to the development of the object database systems. Based on the same general structure and concepts as the multidimensional systems, these new systems allowed the user to store objects directly in the database. That is, the programming constructs being used in the object oriented (OO) programming world

would be used directly in the databases, instead of first being converted to some form of format. Adding support to various OO languages re-created the multidimensional system as object databases.

3.2 Description of DBMS

A DBMS can be an extremely complex set of software programs that controls the organization, storage and retrieval of data (fields, records and files) in a database. It also controls the security of and integrity of database. The DBMS accepts requests for data from the application program and instructs the operating system to transfer the appropriate data.
When a database is used, information system can be changed much more easily as the organization's information requirement changes. New categories of data can be added to the database without disruption to the existing system. Data security prevents unauthorized users from viewing or updating the database. Using passwords, users are allowed access into the entire database or subsets of the database called subschemas. For example an employees' database can contain all the data about an individual employee, but one group of users may be authorized to view only payroll data, while others are allowed access to only work history and medical data.

The DBMS can maintain the integrity of the database by not allowing more than one user to update the same record at the same time. The DBMS can keep the duplicate records out of the database; for example no two customers with the same numbers (key fields) can be entered into the database.

Database query language and report writers allow users to interactively interrogate the database and analyze its data.

If the database provides a way to interactively enter and update database, as well as interrogate it, this capability allows for managing personal databases. However, it may not leave an audit trail of actions or provide the kinds of control necessary in a multi-user organization. These controls are only available when a set of application programs are customized for each data entry and updating function.

Design: A business information system is made up of subjects (customers, employees, vendors, etc) and activities (orders, payments, purchases, etc). Database design is the process of organizing this data into record types and getting the record types to relate to each other. The DBMS should mirror the organization data structure and process transaction efficiently.

Organizations may use one kind of DBMS for daily transaction processing and then move the detail onto another computer that uses DBMS better suited for random inquiries and analysis. Overall data administrators and system analysts perform system design decisions. Database administrators perform detailed database design.

Organizations: The three most common organizations are hierarchical, network and relational models. A database management system may provide one, two or three methods. Inverted lists and other methods are also used. The most suitable structure depends on the application and on the transaction rate and the number of inquiries that will be made.

The dominant model in use today is the relational model, usually used with the SQL query language.

Database servers; these are usually designed computers that hold actual databases and run only the DBMS and related software. Database servers are usually multiprocessors computers with RAID disk arrays used for stable storage. Connected to one or more servers via a high-speed channel, hardware database accelerators are used in large volume transaction processing environments.

Database programs for personal computers come in many shapes, sizes and variation. The same companies that make popular spreadsheet, word processing and other software develop some popular PC database programs. Among the mainstream database program includes dBase, Paradox, Access, FoxPro, Lotus Approach and Filemaker. Others include Oracle, Ingres, Informix and OS/2.

3.3 Database Structure

A typical database consists of tables, fields and records and they play collective roles in a DBMS.

Table: A table is the collection of similar data. It is also though erroneously, known as a database. It is arranged into rows and columns with each entry of data appearing in separate rows and columns.

Record: A record is a complete set of related data. Also, the rows of data in a database field are known as records. All the data on a form is all about one particular customer and can be treated as a single unit. When you add a customer to a customer database, you would add a new record. Likewise when you process a sale and generate an invoice a record is added to an invoice database.

Fields: A field is a property or characteristic that holds information about an entity. On a database table the field is the column of the table. The field of a database separates the type of information contained in that table. For example, each record in the customer table has a name, address and phone number, and each field exists in every record. The person who creates the table defines field.

Types of Field

Different database management systems offer a variety of field types. The most commonly used field types are discussed below.

(i) Text Field: A text field is a string of alphanumerical characters. A text field may contain a person's name, a company name, an address or any other meaningful textual information. A text field can also be used for numbers, but it threats them as just a string of digits, rather than a number.

(ii) Numerical/Currency Field: Numerical (number) fields hold numbers. With most programs, you can select a display format for numbers. The actual number in the field does not contain any formatting, but when the program displays the number it can add a coma separator between thousands and millions, display or not display precision to the right of the precision point, and include other special characters such as naira/dollars sign.

A currency field is a number field with the display format set up by the software to represent money. A currency field displays its values with comma separators, two decimal places or precision for kobo/cent and sometimes a naira/dollar sign.

(iii) Date and Time Fields: Date fields and time fields are specialized fields. When you enter date and time field into Date/Time field, the DBMS accepts your input in the format of date or time, but converts it into a number before storing it in the database. In addition to converting dates to numbers for storage and computational ease, most DBMS products provide automatic error checking for date and time.

(iv) Logical Fields: A logical field (sometimes called Yes/No field) is a field that can hold one or two values. Logical fields can be used for any type of data where there are only two possible values, although the description you give for the choices are unlimited (Yes or No, True or False, Male or Female, Retail or Wholesale).

(v) Memo Fields: A memo field is a special field that can contain information of variable length. A memo field can look like a regular text field that scrolls to the left and the right.

3.4 Functions of DBMS

The following are the basic functions of any database system management

- The DBMS provides the interface between the user and the database program.
- The DBMS maintains the database. This it does by adding new records, deleting dead records and amending records.
- The DBMS expands databases by adding new sets of records or new data to existing records.
- The DBMS provides facilities for different types of processing. It can:

(i) process a complete file (serially or sequentially)
(ii) process required records (selective, sequential or randomly)
(iii) retrieve individual records.

- The DBMS also has the function of providing security for the data in the base. The main aspects are:

(i) protecting data against unauthorized access
(ii) safeguarding data against corruption
(iii) providing recovery and restart facilities after a hardware or software failure.

- The DBMS keeps statistics of the use made of the data in the database. This allows redundant data to be removed. It also allows data frequently used to be kept in readily accessible form so that time is saved.
- The DBMS provides quick access to data especially when it is running on a powerful hardware.
- The DBMS provides easy and quick manipulation of data. Today, the ability to change the organization of data or to edit individual data is what makes using an electronic DBMS appealing.
- The DBMS also provides a means to join (or relate) data in separate database. For example, you can quickly analyze the types of products a customer purchases most often by relating customer information and orders information.
- Data backup and recovery.

3.5 Sorting Data in DBMS

One of the most powerful features of DBMS is its ability to sort information either for a printed report or for you to browse through on the computer's screen. DBMS uses keys or indexes to produce sorted data.

The Primary Key: A primary key defines a default (standard) sort order in which the records of a table are displayed on the screen or printed in a report if no alternative order is specified. A primary key is usually associated with a single field in a table (such as a customer ID number) and values that you enter into that field must be unique – different for every record in the table. Defining a customer number field as the primary key will prevent users from inadvertently entering duplicate entries (two customers with same ID).

The Segmented Key: The primary key of a table can also be made up to more than a single field. This type of primary key is called a segmented key. For example, the primary key can contain three segments – Surname, First Name and Middle initial. With this arrangement, the default (standard) sort order of the table will be primarily by surname, and first name and/or the middle name will sort each identical surname records.

Indexes: Index in a database is a key other than the primary key used for sorting and to speed up searches. It is essentially the same as a key. It can be added to the primary key. For example, though you may use the customer ID as the primary key, however sometimes you may want to print out a customer list that is sorted by company name, city or by some other field. To do this you define an index for the field you want to sort on.

3.6 Database Administrator (DBA)

Database Management System (DBMS) is so important in an organization that a special manager is often appointed to oversee its activities. The database administrator is responsible for the installation and coordination of DBMS. It is responsible for managing one of the most valuable resources of any organization, its data.

The DBA administrator must have a sound knowledge of the structure of the database and of the DBMS. The DBA must be thoroughly conversant with the organization, its system and the information need of managers.

The Basic Functions and Duties of DBAs are as follows:

(i) Overall design and coordination
(ii) To ensure that the database meets the information need of the organization
(iii) To see to it that the facilities for retrieving data and for structuring reported are appropriate to the needs of the organization
(iv) Development of data dictionary
(v) Producing manuals for users describing the facilities the database offers and how to make use of there facilities
(vi) Supervising the addition of new data. For this purpose, the DBA will have to liaise with the managers who use the data and system analysts and programmers who develop the systems.
(vii) System and user documentation
(viii) Interface with users and managers
(ix) Education and training concerning the database
(x) Periodic appraisal of the data held in the base to ensure that it is complete, accurate and not duplicated
(xi) Establishing emergency procedures in the case of system failures or natural or man-made disasters
(xii) Ensuring security and maintaining privacy in the database.

During the initial stages of database designs and selection, a number of important points should be stressed. These points can prevent potential problems while capitalizing on the advantages of a database system. Some of the general guidelines to be used in setting up the database management system include the following:

• The important aspects or needs of the organization must be stressed
• Involvement of the database users
• Determine the initial records and fields to be placed on the database
• Business problems need to be stressed
• Review database needs and requirements

Data security and invasion of privacy problems should be tackled early in the design and set up of a DBMS; most DBMS have excellent procedures and techniques to protect individual privacy and maintain data security. These procedures and techniques should be fully used.

Training is another critical issue in the successful implementation and the use of DBMS. In addition to a database administrator, technical staff as competent data processing personnel (to create, manage and maintain the database, training programmes) are needed to alert managers and other decision-makers to the potential use of the system.

4.0 CONCLUSION

Data is considered the bedrock of any organization and an orderly arrangement of the data goes a long way to determine the efficiency of such an organization. However, without orderly arrangement of data it becomes difficult to access such data. DBMS programs have made access of data much easier.

As we experience continual growth in data churned out by corporations, program writers are equally working hard to meet the challenges posed by this growth of data.

5.0 SUMMARY

In summary, this unit of the course has highlighted the following points for your review:

- A database management system (DBMS) is tool computer use for the orderly processing, storage and retrieval of data. It is the programme or collection of programs that allow users (and other programs) to access and work with a database anytime.

- Among the mainstream database programs are D Base, Paradox, Access, FoxPro, Lotus Approach and Filemaker. Others are Oracle, Ingres, Informix and OS/2.

- Data Redundancy is the storage of the same data in multiple tables. For example, if a person's address and phone numbers were to be stored in more than one table, the address and phone number would be considered as redundant data.

- A typical database consists of tables, fields and records and they play collective roles in a DBMS.

- The DBMS provides the interface between the user and the database program.

- The DBMS maintains the database. This it does by adding new records, deleting dead records and amending records.

- The DBMS expands databases by adding new sets of records or new data to existing records.

- One of the most powerful features of DBMS is its ability to sort information either for a printed report or for you to browse through on the computer's screen. DBMS uses keys or indexes to produce sorted data.

- Defining a customer number field as the primary key will prevent users from inadvertently entering duplicate entries (two customers with same ID).

- Database Management System (DBMS) is so important in an organization that a special manager is often appointed to oversee its activities. The database administrator is responsible for the installation and coordination of DBMS.
- During the initial stages of database designs and selection, a number of important points should be stressed. These points can prevent potential problems while capitalizing on the advantages of a database system.

- Data security and invasion of privacy problems should be tackled early in the design and set up of a DBMS; most DBMS have excellent procedures and techniques to protect individual privacy and maintain data security.

6.0 TUTOR-MARKED ASSIGNMENT

1. Mention 10 basic functions of database administrator in an organization.
2. Briefly discuss the evolution of DBMS.

7.0 REFERENCES/FURTHER READINGS

Anderson, R.G (1994). Data Processing: Principles & Practice, Vol. 1. Pitman Publishing.

Anderson, R.G (1994).Data Processing: Information Systems & *Technology, Vol. 2. Pitman Publishing.*

French, C.S. (1993). Computer Studies. DP Publishing Ltd.

Norton, P (1995). Introduction to Computers. Macmillan/McGraw-Hill.

UNIT 5 OPERATING SYSTEMS

CONTENTS

1.0 INTRODUCTION

The computer is a machine that can understand only electrical impulses; the user gives the instructions in language not understood by the computer and therefore there is a gap top be bridged. This bridging is done by special software known as the Operating System (OS). This software is the only interface that the user has with the computer. When a user specifies a job to the computer it is actually given to the operating system. The working details are then taken over by the OS.

An operating system (OS) is itself a computer program. However, it is a very important one on a computer. Otherwise an OS is defined as a suite of program which takes control over the operation of the computer to the extent of being able to allow a number of programs to be run on the computer without human intervention by an operator. Operating system software works in the background to create a working environment for your personal computer. The OS sets the rule for how the computer and application program work together. The OS makes the computer to recognize the CPU, memory, keyboard, video display system and disk drives.

In addition it provides the facility for the user to communicate with the computer and it serves as a platform on which to run application programs.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- define an operating system
- explain the various functions of an operating system in relation to the working of a computer
- differentiate the categories of operating systems
- state the advantages and disadvantages associated with types of operating systems.

3.0 MAIN CONTENT

3.1 Functions of Operating Systems

The OS has four to five primary functions:

1. **Booting of Computer: This is the first process which takes place the** moment the computer's electrical switch is put on. During this process all the peripherals connected to the computer are checked and validated; at the end of the validation process, the OS signals the user to begin working on the computer.

2. **Providing User Interface: The OS provides an interface for the user, either as a command line interface or as a graphical user** interface. This enables the user to communicate with the computer. .

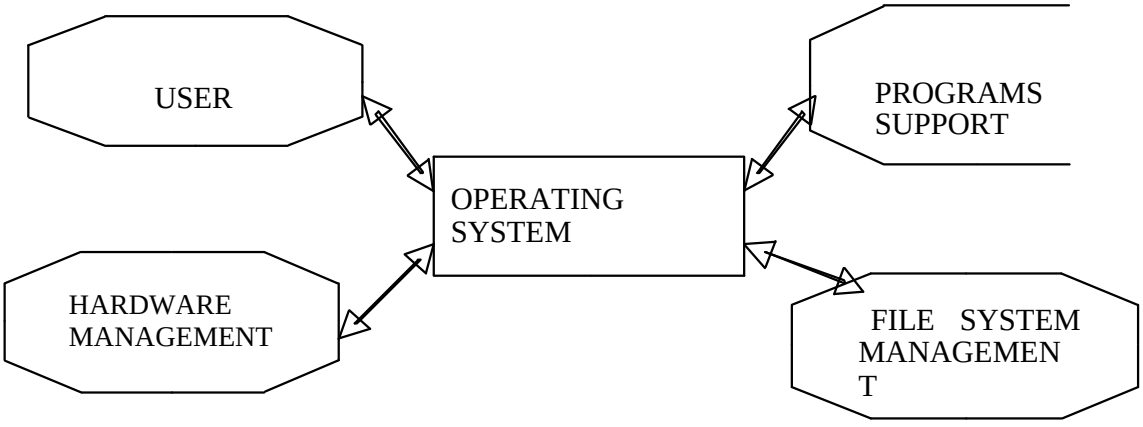


Fig 4: Applications of the operating system

In other words OS communicates with the computer user or operator by means of terminals and through the use of monitor command responses. The user may also be able to communicate with the OS by means of command language.

There are two broad categories of interfaces: command – line **interfaces and graphical user interfaces. To use an OS with a** command – line interface, you type words and symbols on the keyboard.

With a graphical user interface (GUI) you select actions by using a mouse or similar pointing device to click on pictures called icons or to pick options from menus. Every OS provides a user interface, whether it is made up of text or is graphical in nature. For example, DOS (Disk Operating System) the most widely used OS in the world has a command – line interface which means the user controls the program by typing commands at a prompt. On the other hand, the Windows OS use the graphic user interface to control programs.

3. **Managing the Hardware: OS controls and manages hardware** resources. For example, OS manages the selection and operation of devices used for input, output and storage. In other words the OS serves as the intermediary between programs and hardware.

Regardless of the type of user interface, the OS intercepts commands to use memory and other devices, keeping track of what programs have access to what devices and so on. For example if you tell the OS to list the files in a directory or folder, the software interpreting the command, sends a request to the CPU in form of interrupting the CPU and instructing the CPU to go to the disk drive and retrieve the names of the files it finds in the directory or folder.

4. **Managing the File System: The operating system groups data** together into -logical compartments for storage on disk. These groups of data are called files. The computer stores information in files. Files may contain program instructions or data created or used by a program. The OS maintains the list of files on a disk.

5. **Supporting Programs: Another major function of an OS is to** provide services to other programs. Often these services are similar to those that the OS provides directly to users. For example when you want your word- processing program to retrieve a document, the word processor will list the files in the directory that you specify.

To do this, the program (word – processing) call on the OS to list the files. The OS goes through the same process to build a list of files whether it receives instruction directly from a user or from an application program. But when the request comes from an application the OS sends the result of its work to the application program instead of directly to the computer screen.

Some of the other services that an OS provides to programs are:

- saving files to disk reading them from disk into memory
- checking available disk or memory space
- allocating memory to hold data for a program

- reading keystrokes from the keyboard
- displaying characters or graphics on the screen.
- loading the user program into memory
- giving instruction to display the result on the monitor

3.2 Categories of Operating Systems

Operating systems are designed with many objectives in mind. Among the most basic questions in OS design are the following:

- Should the OS be able to do more than one thing at a time?
- Should the OS support only one user or should it support multiple users simultaneously?
- Should the OS be able to use more than one CPU?

1. Multitasking the Operating System/Multi Programming

This is an OS that is able to run more than one program at a time. There are two types of multitasking operating systems- cooperative and preemptive.

(a) Cooperative Multitasking: This requires cooperation between the OS and application programs. In this case the programs are written in such a way that they periodically check with the OS to see whether any other program needs the CPU. If a program needs the CPU, they relinquish control of the CPU to the next program. Cooperative multitasking is common with Macintosh OS and DOS computers running Microsoft Windows.

(b) Preemptive Multitasking: Under this scheme, the OS maintain a list of processes (programs) that are running. Each process on the list is assigned a priority by the OS when it is started. At any time, the OS can intervene and modify the priority list. The OS also retains control of the amount of time that it spends with any process before going to the next process.

Unix, OS/2 and Windows NT employ preemptive multitasking.

2. Multi-user Operating Systems

A multi-user OS allows more than a single user access to a computer at the same time. Of course, to accomplish this, a multi-user OS must also be capable of multitasking. Only UNIX OS and Windows NT are capable of supporting multiple users.

UNIX provides three ways to let people use the same PC at the same time.

a) The first way to connect to a PC running UNIX is from another computer with a modem. The remote user can log in and run programs, list files, send e-mails read the news and otherwise do everything they could do if they were physically in front of the UNIX computer.

b) The second way to connect to a UNIX computer is by attaching terminals to the PC. Terminals are inexpensive devices that consist of a keyboard, and a monitor.

c) The third way to tap into a UNIX computer multi-user capabilities is with a network.

The typical DOS network is a collection of independent PCs that can share common resources, including a large hard disk. But they are still single-user single-tasking computers – one network user cannot run a program on another PC on the network (even if no one is using it).

With a UNIX computer on a network, you can use virtually any type of computer to connect across the network to the UNIX machine.

3. Multiprocessing Operating Systems

A special type of OS is required to use a computer equipped with more than one CPU. In other words, multiprocessing requires an OS capable of using and managing a series of CPUs. There are two types.

With asymmetrical multiprocessing one main CPU retains the overall control of the computer as well as that of the other microprocessor. On the other hand in symmetrical multiprocessing there is no single controlling CPU. This arrangement provides a linear increase in system capacity for each processor added to the system.

Some extensions of UNIX supports asymmetric multiprocessing while Windows NT supports symmetric multiprocessing.

3.3 Types of Operating Systems

There are different types of personal operating systems with their unique characteristics, advantages and disadvantages.

1. DOS (Disk Operating System)

MS-DOS used to be the most common and most popular of all the PC operating systems. The reason for its popularity then is because of the

overwhelming volume of available software and large installation of Intel-based PCs. DOS runs on any of the Intel microprocessor. DOS functions through the command–line interface i.e. DOS functions by commands. The DOS provides less than 3MB of disk space. Some Examples of common DOS commands are:

Command	Purpose
DIR	Display a directory listing
COPY	Copies a file
RENAME or REN	Rename a file
DEL or ERASE	Erase a file
CHDIR or CD	Changes the current directory
MKDIR	Make a new directory
FORMAT	Formats a disk

Advantages of DOS

- It is the most popular microcomputer operating system ever sold
- It supports enormous number of applications program
- It is relatively easy to install and use.

Disadvantages of DOS

- DOS file names is limited to eight characters, plus a three-character extension. No major OS places this restriction on its users.
- DOS was designed for the 16-bit CPUs that Intel was making in the early and middle 1980s. It can't take advantage of the 32-bit architecture of the 386,486, and Pentium chips.
- DOS was not designed to handle a large amount of RAM that today's PCs typically use. As a result utilities are required to access memory beyond the 1-MB limit imposed by DOS
- It uses only character/command line interface
- Application programs running on DOS have direct access to only 640 kb of primary storage
- DOS can only do single tasking (i.e. support only one user and one application program at the same time), although recent versions can task switch (interrupt one program to do another)

2. Microsoft Windows

Microsoft Windows is a version of DOS. It was released in 1987.It is the biggest thing to happen to DOS.

Microsoft Windows can run standard DOS programs either in a window within the Graphic Use Interface (GUI) or on a full-screen. To take full

advantage of the Microsoft environment you need programs written for Microsoft Windows. The Windows program provides 10MB of disk space, 2MB Random Access Memory (RAM) with greater than 4MB for application.

Advantages of Microsoft Windows

The advantages of Microsoft Windows are several and they include the following:

- It is easier for new computer users to learn to use a mouse, icons, and drop down menus than it is to learn the use of command-line OS, that is, graphic user interface is provided.
- A Microsoft Windows word processor works the way a Microsoft Windows spreadsheet (or any other Windows program) works.
- Microsoft Windows allows users to switch between running programs quickly and easily, that is multitasking
- A file name can be up to 256 characters
- Dynamic Data Interchange is available. With two or more applications running at the same time, data and results can be shared back and forth.
- There is more primary storage access.

Disadvantages of Microsoft Windows

- Effective use requires t least 80386 microprocessors, four times as much memory as DOS and a hard disk
- It has limited network capabilities
- It makes unrecoverable errors, a problem with earlier versions although most recent versions are much better.

On the other hand too, unfortunately not every PC is an ideal candidate for Microsoft Windows because it requires a fairly fast and capable computer – and, to realize the most benefit from the graphic environment, the computer should also have a fast, high-resolution monitor.

3. Operating Systems 2 (OS/2)

1BM and Microsoft teamed up to develop the Operating System 2(OS/2) to take full advantage of the multitasking capabilities of the newly introduced Intel 80286 microprocessor. OS/2 like DOS has a character–based command-line mode, but unlike DOS, the command interpreter is a separate program from the OS kernel and is only involved when you click on the OS/2. OS/2 runs only on Intel 80286 and later processors. It is a multi-tasking system.

OS/2 commands are similar to those of DOS. Others differ only slightly and of course OS/2 has more command because OS/2 is larger, more comprehensive and more modern. Workplace shell is the graphical environment for OS/2.

Advantages of OS/2

- It supports multitasking
- Dynamic Data Interchange is available
- Graphic user interface is consistent
- It provides more primary storage facilities
- Networking capability to link users sharing information is available
- There is flexibility to adjust to changing demands and processing efficiency.

Disadvantages of OS/2

- There are far fewer users than DOS or Windows
- Supports/available for fewer specialized application programs
- Effective use requires at least an 80386 microprocessor, twice the memory and disk space required for Windows.

4. The Macintosh OS

The Macintosh OS is a purely graphic machine. In fact there is no equipment of a command-line interface available for it. Its tight integration of OS, GUI and desktop make it desirable for people who do not want to deal with a command-line interface. The Macintosh OS only runs on Macintosh machine. The Macintosh OS has an additional network protocol built into it and is ideal for desktop publishing. Installing and configuring a Macintosh with new hardware device is simple.

Advantages of Macintosh

- It offers high standards for graphic processing
- It is easy to learn
- It has a consistent graphic user interface with all applications
- It can do multitasking
- It can share data with other applications i.e. Dynamic Data Interchange.

Disadvantages of Macintosh

- Initially most corporate buyers do not view Macintosh as a serious business application
- Programs written for DOS will not run on a Macintosh unless specialty hardware and software have been imposed.

5. UNIX

UNIX is the first OS that runs on many different types of computers. It runs on Cray supercomputers, PCs, and everything in between including mainframes and minicomputers.

UNIX is older than all the other PC operating systems and in many ways served as a model for them. UNIX is based on a simple idea-small is better. Every command and program that makes up the OS is designed to do a simple very specific task and do it well. UNIX is an extremely robust and capable OS that utilizes command –line and there are so many commands.

Advantages of UNIX

- It provides multitasking facilities
- It allows multi-users to share computers simultaneously
- It is not limited to primary storage devices
- It is excellent in networking

Disadvantages of UNIX

- Fewer business application programs are presently available
- No one UNIX standard exists
- There is no standard graphic user interface
- Security can be a problem because UNIX is an open system.

6. Microsoft Windows NT

Microsoft Windows NT is a new OS designed from scratch for the most modern and capable machines available. Microsoft Windows NT offers built-in features that no other PC OS has – with the possible exception of UNIX. In addition to the traditional UNIX features of strict system security, built-in networking, built-in communications and electronic mail services development and system administration tools, and a GUI. Microsoft Windows NT can run Microsoft Windows applications and many UNIX applications, directly.

Like OS/2 it is a 32-bit OS that can use 386, 486 and Pentium processors Microsoft Windows NT is multitasking and purely graphical OS with network software to make a network client or server. It is single- user and allows access to command line interface of the DOS unlike the Macintosh.

4.0 CONCLUSION

The operating system is the backbone of the operation of any computer system because it is responsible for laying the foundational instruction on which other classes of programs function. The operating system market is very dynamic, which is typical of the information technology age. Different types are written to meet the increasing needs in the business world.

5.0 SUMMARY

- The computer is a machine that can understand only electrical impulses; the user gives the instructions in language not understood by the computer and therefore there is a gap to be bridged. This bridging is done by special software known as the Operating System (OS).

- A multi-user OS allows more than a single user access to a computer at the same time.

- MS-DOS used to be the most common and most popular of all the PC operating systems. The reason for its popularity then is because of the overwhelming volume of available software and large installation of Intel-based PCs.

- Microsoft Windows is a version of DOS. It was released in 1987.It is the biggest thing to happen to DOS.

- 1BM and Microsoft teamed up to develop the Operating System 2(OS/2) to take full advantage of the multitasking capabilities of the newly introduced Intel 80286 microprocessor.

- The Macintosh OS is a purely graphic machine. In fact there is no equipment of a command-line interface available for it.

- UNIX is the first OS that runs on many different types of computers. It runs on Cray supercomputers, PCs, and everything in between, including mainframes and minicomputers.

- Microsoft Windows NT is a new OS designed from scratch for the most modern and capable machines available.

6.0 TUTOR-MARKED ASSIGNMENT

1. Briefly discuss the advantages and disadvantages of an OS/2 operating system.
2. Identify the factors responsible for the seemingly failure of DOS program.

7.0 REFERENCES/FURTHER READINGS

French, C.S (1993).Computer Studies. DP Publishing Ltd.

Norton, (1995). Introduction to Computers. Macmillan/McGraw-Hill.

Ron, W (1995). How Computer Works. Macmillan Computer Publishing.

UNIT 6 COMPUTER SYSTEM SECURITY

CONTENTS

1.0 INTRODUCTION

Computer security is a field of computer science concerned with the control of risk related to computer use. Computer security can be seen as a subfield of security engineering, which looks at broader security issues in addition to computer security.

In a secure system the authorised users of that system are still able to do what they should be able to do. One might be able to secure a computer beyond misuse using extreme measures:

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts. However, this would not be regarded as a useful secure system.

It is important to distinguish the techniques used to increase a system's security from the issue of that system's security status. In particular, systems which contain fundamental flaws in their security designs cannot be made secure without compromising their usability. Consequently, most computer systems cannot be made secure even after the application of extensive "computer security" measures. Furthermore, if they are made secure, often it is to the detriment of usability.

The early Multics operating system was notable for its early emphasis on computer security by design, and Multics was possibly the very first operating system to be designed as a secure system from the ground up. In spite of this, Multics' security was broken, not once, but repeatedly. The strategy was known as 'penetrate and test' and has become widely known as a non-terminating process that fails to produce computer

security. This led to further work on computer security that prefigured modern security engineering techniques producing closed form processes that terminate.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- explain what computer security is
- identify security techniques for securing information
- design a security system
- differentiate network security from computer security.

3.0 MAIN CONTENT

3.1 Secure Operating System Context

One context of the term computer security is its use pertaining to a technology to implement a secure operating system. Much of this technology is based on science developed in the 1980s and used to produce what may be some of the most impenetrable operating systems ever. Though still valid, the science did not change, the technology is almost inactive today, perhaps because it is complex or not widely understood. Such ultra strong secure operating systems are based on operating system kernel technology that can guarantee that certain security policies are absolutely enforced on an operating environment. An example of such a security policy is the Bell-LaPadula model.

The strategy is based on a coupling of special microprocessor hardware features, often involving the Memory Management Unit, to a special correctly implemented operating system kernel. This forms the foundation for a secure operating system that if certain critical parts are designed and implemented correctly can ensure that it is physically impossible for arbitrarily hostile or intelligently subversive applications to violate the security policy. This amazing capability is enabled because they not only impose a security policy, but they also completely protect themselves from corruption. Ordinary operating systems lack the completeness property in this latter capability. The design methodology to produce such secure systems is not an ad-hoc best effort activity, but one that is very precise, deterministic and logical.

Systems designed with such methodology represent the state of the art of computer security and the capability to produce them is not widely known. In sharp contrast to most kinds of software, they meet specifications with verifiable certainty comparable to specifications for size, weight and power. Secure operating systems designed this way are

used primarily to protect national security information and military secrets. These are very powerful security tools and very few secure operating systems have been certified at the highest level (Orange Book A-1) to operate over the range of Top Secret to unclassified (including Honeywell SCOMP, USAF SACDIN, NSA Blacker and Boeing MLS LAN.) The assurance of security depends not only on the soundness of the design strategy, but also on the assurance of correctness of the implementation, and therefore there are degrees of security strength for COMPUSEC. The Common Criteria quantifies security strength of products in terms of two orthogonal components, security capability (as Protection Profile) and assurance levels (as EAL levels.) For reasons that are the subject of another article, none of these ultra high assurances secure general purpose operating systems have been produced for decades or certified under the Common Criteria.

3.2 Computer Security by Design

Computer security is a logic-based technology. There is no universal standard notion of what secure behavior is. "Security" is a property that is unique to each situation and so must be overtly defined if it is to be seriously enforced, defined by a Security Policy. Security is not an ancillary function of a computer application, but often what the application doesn't do. Unless the application is just trusted to be 'secure,' security can only be imposed as a constraint on the application's behavior from outside of the application. There are several approaches to security in computing; sometimes a combination of approaches is valid:

Trust all the software to abide by a security policy but the software is not trustworthy (this is computer insecurity).

Trust all the software to abide by a security policy and the software is validated as trustworthy (by tedious branch and path analysis for example).

Trust no software but enforce a security policy with mechanisms that are not trustworthy (again this is computer insecurity).

Trust no software but enforce a security policy with trustworthy mechanisms.

Many approaches unintentionally follow 1. Obviously, 1 and 3 lead to failure. Since 2 is expensive and non-deterministic, its use is very limited. Because 4 is often hardware-based mechanisms and avoid abstractions and a multiplicity of degrees of freedom, it is more

practical. Combinations of 2 and 4 are often used in a layered architecture with thin layers of 2 and thick layers of 4.

There are a variety of strategies and techniques used to design in security. There are few, if any strategies to add on security after design. Some of the strategies to design in security are discussed in this section.

One technique enforces the principle of least privilege to great extent, where an entity has only the privileges that are needed for its function. That way, even if an attacker has subverted one part of the system, fine-grained security ensures that it is just as difficult for them to subvert the rest.

Furthermore, by breaking the system up into smaller components, the complexity of individual components is reduced, opening up the possibility of using techniques such as automated theorem proving to prove the correctness of crucial software subsystems. This enables a closed form solution to security that works well when only a single well-characterized property can be isolated as critical, and that property is also assessable to math. Not surprisingly, it is impractical for generalized correctness, which probably cannot even be defined, much less proven. Where formal correctness proofs are not possible, rigorous use of code review and unit testing represent a best-effort approach to make modules secure.

The design should use "defense in depth", where more than one subsystem needs to be compromised to compromise the security of the system and the information it holds. Defense in depth works when the subverting hurdle is not a platform to facilitate the subverting of another platform. Also, the cascading principle acknowledges that several low hurdles do not make a high hurdle. So cascading several weak mechanisms does not provide the safety of a single stronger mechanism.

Subsystems should default to secure settings, and wherever possible should be designed to "fail secure" rather than "fail insecure". Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure. What constitutes such a decision and what authorities are legitimate is obviously controversial.

In addition, security should not be an all or nothing issue. The designers and operators of systems should assume that security breaches are inevitable in the long term. Full audit trails should be kept from system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering

their tracks. Finally, full disclosure helps to ensure that when bugs are found the "window of vulnerability" is kept as short as possible.

3.3 Techniques for Creating Secure Systems

The following techniques can be used in engineering secure systems. These techniques, whilst useful, do not of themselves ensure security. One security maxim is "a security system is no stronger than its weakest link".

Automated theorem proving and other verification tools can enable critical algorithms and code used in secure systems to be mathematically proven to meet their specifications.

Thus simple microkernels can be written so that we can be sure they don't contain any bugs: eg EROS and Coyotos.

A bigger OS, capable of providing a standard API like POSIX, can be built on a microkernel using small API servers running as normal programs. If one of these API servers has a bug, the kernel and the other servers are not affected: eg Hurd.

Cryptographic techniques can be used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.

Strong authentication techniques can be used to ensure that communication end-points are who they say they are.

Secure cryptoprocessors can be used to leverage physical security techniques into protecting the security of the computer system.

Chain of trust techniques can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.

Mandatory access control can be used to ensure that privileged access is withdrawn when privileges are revoked. For example, deleting a user account should also stop any processes that are running with that user's privileges.

Capability and access control list techniques can be used to ensure privilege separation and mandatory access control. The next sections discuss their use.

Don't run an application with known security flaws. Either leave it turned off until it can be patched or otherwise fixed, or delete it and

replace it with some other application. Publicly known flaws are the main entry used by worms to automatically break into a system and then spread to other systems connected to it. The security website Secunia provides a search tool for unpatched known flaws in popular products.

Cryptographic techniques involve transforming information, scrambling it so it becomes unreadable during transmission. The intended recipient can unscramble the message, but eavesdroppers cannot.

Backups are a way of securing your information; they are another copy of all your important computer files kept in another location. These files are kept on hard disks, CD-Rs, CD-RWs, and tapes. Backups can be kept in a multitude of locations, some of the suggested places would be a fireproof, waterproof, and heat proof safe, or in a separate, offsite location than that in which the original files are contained. Some individuals and companies also keep their backups in safe deposit boxes inside bank vaults. There is also a fourth option, which involves using one of the file hosting services that backs up files over the Internet for both business and individuals.

Backups are also important for reasons other than security. Natural disasters, such as earthquakes, hurricanes, or tornadoes, may strike the building where the computer is located. The building can be on fire, or an explosion may occur. There needs to be a recent backup at an alternate secure location, in case of such kind of disaster. The backup needs to be moved between the geographic sites in a secure manner, so as to prevent it from being stolen.

Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

Firewalls are systems which help protect computers and computer networks from attack and subsequent intrusion by restricting the network traffic which can pass through them, based on a set of system administrator defined rules.

Access authorization restricts access to a computer to group of users through the use of authentication systems. These systems can protect either the whole computer - such as through an interactive logon screen - or individual services, such as an FTP server. There are many methods for identifying and authenticating users, such as passwords, identification cards, and, more recently, smart cards and biometric systems.

Encryption is used to protect your message from the eyes of others. It can be done in several ways by switching the characters around,

replacing characters with others, and even removing characters from the message. These have to be used in combination to make the encryption secure enough that is to say, sufficiently difficult to crack. Public key encryption is a refined and practical way of doing encryption. It allows for example anyone to write a message for a list of recipients, and only those recipients will be able to read that message.

Intrusion-detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.

Social engineering awareness - Keeping yourself and your employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of your network and servers.

3.4 Network Security

Network security consists of the provisions made in an underlying network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together.

How different is it from computer security? In plain words, securing any network infrastructure is like securing possible entry points of attacks on a country by deploying appropriate defense. Computer security is more like providing means of self-defense to each individual citizen of the country. The former is better and practical to protect the civilians from getting exposed to the attacks. The preventive measures attempt to secure the access to individual computers--the network itself--thereby protecting the computers and other shared resources such as printers, network-attached storage connected by the network. Attacks could be stopped at their entry points before they spread. As opposed to this, in computer security the measures taken are focused on securing individual computer hosts. A computer host whose security is compromised is likely to infect other hosts connected to a potentially unsecured network. A computer host's security is vulnerable to users with higher privileges to those hosts.

Network security starts from authenticating any user. Once authenticated, firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the

network. An intrusion prevention system (IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.

Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used to further tighten security of the actual network being protected by the honeypot.

4.0 CONCLUSION

Coming advances in computation will no doubt produce new security problems. Also, though advances in technology may change some features of security, it will continue to be true that information security must be seen as a human problem. Management must be involved. Without higher level management support, there will be insufficient budgets for and insufficient attention paid to information security. Without sufficient budgets, necessary control measures will not be made. Without sufficient management attention, control of decisions that need to be made will be ignored.

5.0 SUMMARY

- Computer security is a field of computer science concerned with the control of risk related to computer use. Computer security can be seen as a subfield of security engineering, which looks at broader security issues in addition to computer security.

- One context of the term computer security is its use pertaining to a technology to implement a secure operating system. Much of this technology is based on science developed in the 1980s and used to produce what may be some of the most impenetrable operating systems ever.

- Computer security is a logic-based technology. There is no universal standard notion of what secure behavior is. “Security” is a property that is unique to each situation and so must be overtly defined if it is to be seriously enforced, defined by a Security Policy.

• In addition, security should not be an all or nothing issue. The designers and operators of systems should assume that security breaches are inevitable in the long term. Full.

• Cryptographic techniques involve transforming information, scrambling it so it becomes unreadable during transmission. The intended recipient can unscramble the message, but eavesdroppers cannot.

• Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

• Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and the effectiveness (or lack) of these measures combined together.

6.0 TUTOR-MARKED ASSIGNMENT

1. Differentiate computer security from network security.
2. Mention 5 computer security measures.

7.0 REFERENCES/FURTHER READINGS

Anderson, Ross J. Security Engineering: A Guide to Building *Dependable Distributed Systems.*

Bruce, Schneier Secrets & Lies: Digital Security in a Networked World.

Seacord, Robert C. (2005). Secure Coding in C and C++. Addison Wesley, September.

Karger, Paul A. & Schell, Roger R. Thirty Years Later: Lessons from *the Multics Security Evaluation, IBM white paper.*

Stoll, Clifford. Cuckoo's Egg: Tracking a Spy through the Maze of *Computer Espionage. Pocket Books.*

Haag, Stephen; Cummings, Maeve; McCubbrey, Donald; Pinsonneault, Alain; Donovan, Richard. Management Information Systems for *the Information Age.*

Neumann, Peter G. (2004). Principled Assuredly Trustworthy *Composable Architectures.*

Gasser, Morrie (1998). Building a Secure Computer System.

Lee, E. Stewart (1999) Essays about Computer Security. Cambridge.

Dittrich, Dave. Network Monitoring/Intrusion Detection Systems (IDS) University of Washington. ^ Honeypots, Honeynets

Dekker, Marcel (1997).“Security of the Internet”. The Froehlich/Kent *Encyclopedia of Telecommunications Vol. 15. New York.*

Curtin, Matt. Introduction to Network Security.

Books about Network Security

DeCapite, Duane (2006). Self-Defending Networks: The Next *Generation of Network Security. Cisco Press.*

Tesch, Dale & Abelar, Greg (2006).Security Threat Mitigation and *Response: Understanding CS-MARS. Cisco Press.*

Pepelnjak, Ivan (2006).Deploying Zone-Based Firewalls. Cisco Press.

Kaufman, Radia Perlman & Speciner, Charlie Mike(2002).Network *Security: PRIVATE Communication in a PUBLIC World.* | Prentice-Hall.

UNIT 7 COMPUTER INSECURITY

CONTENTS

1.0 INTRODUCTION

Most current real-world computer security efforts focus on external threats, and generally treat the computer system itself as a trusted system. Some knowledgeable observers consider this to be a disastrous mistake, and point out that this distinction is the cause of much of the insecurity of current computer systems - once an attacker has subverted one part of a system without fine-grained security, he or she usually has access to most or all of the features of that system. Because computer systems can be very complex, and cannot be guaranteed to be free of defects, this security stance tends to produce insecure systems.

The "trusted systems" approach has been predominant in the design of many Microsoft software products, due to the long-standing Microsoft policy of emphasizing functionality and 'ease of use over security. Since Microsoft products currently dominate the desktop and home computing markets, this has led to unfortunate effects. However, the problems described here derive from the security stance taken by software and hardware vendors generally, rather than the failing of a single vendor. Microsoft is not out of line in this respect, just far more prominent with respect to its consumer market share.

It should be noted that the Windows NT line of operating systems from Microsoft contained mechanisms to limit this, such as services that ran under dedicated user accounts, and Role-Based Access Control (RBAC) with user/group rights, but the Windows 95 line of products lacked most of these functions. Before the release of Windows 2003 Microsoft has changed their official stance, taking a more locked down approach. On 15 January 2002, Bill Gates sent out a memo on Trustworthy

Computing, marking the official change in company stance. Regardless, Microsoft's latest operating system Windows XP is still plagued by complaints about lack of local security and inability to use the fine-grained user access controls together with certain software (esp. certain popular computer games).

2.0 OBJECTIVES

At the end of this unit you should be able to:

- view the issue of computer security from another perspective, especially from the negative angle
- examine the financial implications of systems insecurity
- answer the question of the different types of computer attacks
- identify some of the ways to reduce computer insecurity
- examine the security measures to deal with threat and attacks of computer.

3.0 MAIN CONTENT

3.1 Financial Cost of Computer Insecurity

Serious financial damage has been caused by computer security breaches, but reliably estimating costs is quite difficult. Figures in the billions of dollars have been quoted in relation to the damage caused by malware such as computer worms like the Code Red worm but such estimates may be exaggerated. However, other losses, such as those caused by the compromise of credit card information, can be more easily determined, and they have been substantial, as measured by millions of individual victims of identity theft each year in each of several nations, and the severe hardship imposed on each victim, that can wipe out all of their finances, prevent them from getting a job, plus being treated as if *they were the criminal. Volumes of victims of phishing and other scams* may not be known.

Individuals who have been infected with spyware or malware likely go through a costly and time-consuming process of having their computer cleaned. Spyware and malware is considered to be a problem specific to the various Microsoft Windows Operating Systems; however this can be explained somewhat by the fact that Microsoft controls a major share of the PC market and thus represent the most prominent target.

3.2 Forms of Computer Insecurity

There are many similarities (yet many fundamental differences) between computer and physical security. Just like real-world security, the

motivations for breaches of computer security vary between attackers, sometimes called hackers or crackers. Some are teenage thrill-seekers or vandals (the kind often responsible for defacing web sites); similarly, some web site defacements are done to make political statements. However, some attackers are highly skilled and motivated with the goal of compromising computers for financial gain or espionage. An example of the latter is Markus Hess who spied for the KGB and was ultimately caught because of the efforts of Clifford Stoll, who wrote an amusing and accurate book, The Cuckoo's Egg, about his experiences. For those seeking to prevent security breaches, the first step is usually to attempt to identify what might motivate an attack on the system, how much the continued operation and information security of the system are worth, and who might be motivated to breach it. The precautions required for a home PC are very different for those of banks' Internet banking system, and different again for a classified military network. Other computer security writers suggest that, since an attacker using a network need know nothing about you or what you have on your computer, attacker motivation is inherently impossible to determine beyond guessing. If true, blocking all possible attacks is the only plausible action to take.

Vulnerabilities

To understand the techniques for securing a computer system, it is important to first understand the various types of "attacks" that can be made against it. These threats can typically be classified into one of these seven categories:

Exploits

Software flaws, especially buffer overflows, are often exploited to gain control of a computer, or to cause it to operate in an unexpected manner. Many development methodologies rely on testing to ensure the quality of any code released; this process often fails to discover extremely unusual potential exploits. The term "exploit" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in Trojan horses and computer viruses. In some cases, a vulnerability can lie in a certain programs processing of a specific file type, such as a non-executable media file.

Eavesdropping

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system (ie, with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic

transmissions generated by the hardware such as TEMPEST. The FBI's proposed Carnivore program was intended to act as a system of eavesdropping protocols built into the systems of internet service providers.

Social Engineering and Human Error

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them, for example sending messages that they are the system administrator and asking for passwords. This deception is known as Social engineering.

Denial of Service Attacks

Denial of Service (DoS) attacks differs slightly from those listed above, in that they are not primarily a means to gain unauthorized access or control of a system. They are instead designed to render it unusable. Attackers can deny service to individual victims, such as by deliberately guessing a wrong password 3 consecutive times and thus causing the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. These types of attack are, in practice, very hard to prevent, because the behavior of whole networks needs to be analyzed, not only of small pieces of code. Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (commonly referred to as "zombie computers") are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion. Another technique to exhaust victim resources is though the use of an attack amplifier - where the attacker takes advantage of poorly designed protocols on 3rd party machines, such as FTP or DNS, in order to instruct these hosts to launch the flood. There are also commonly vulnerabilities in applications that cannot be used to take control over a computer, but merely make the target application malfunction or crash. This is known as a denial-of-service exploit.

Indirect attacks

Attacks in which one or more of the attack types above are launched from a third party computer which has been taken over remotely. By using someone else's computer to launch an attack, it becomes far more difficult to track down the actual attacker. There have also been cases where attackers took advantage of public anonymizing systems, such as the tor onion router system.

Backdoors

Methods of bypassing normal authentication or giving remote access to a computer to somebody who knows about the backdoor, while intended to remain hidden to casual inspection. The backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing "legitimate" program, or executable file. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports. It may also fake information about disk and memory usage.

Direct Access Attacks

These are common consumer devices that can be used to transfer data surreptitiously. Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media, for instance CD-R/DVD-R, tape; or portable devices such as keydrives, digital cameras or digital audio players. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the harddrive(s) this way. The only way to defeat this is to encrypt the storage media and store the key separate from the system.

3.3 Reducing Vulnerabilities

Computer code is regarded by some as just a form of mathematics. It is theoretically possible to prove the correctness of computer programs (though this is usually too difficult to be practicable outside very limited circumstances) though the likelihood of actually achieving this in large-scale practical systems is regarded as unlikely in the extreme by most with practical experience in the industry.

It is also possible to protect messages in transit (ie, communications) by means of cryptography. One method of encryption —the one-time pad —has been proven to be unbreakable when correctly used. This method was used by the Soviet Union during the Cold War, though flaws in their implementation allowed some cryptanalysis. The method uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message. For transmitted computer encryption this method is difficult to use properly (securely), and highly inconvenient as well. Other methods of encryption, while breakable in theory, are often virtually impossible to directly break by any means publicly known today. Breaking them requires some non-

cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.
Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Even in a highly disciplined environment, such as in military organizations, social engineering attacks can still be difficult to foresee and prevent.

In practice, only a small fraction of computer program code is mathematically proven, or even goes through comprehensive information technology audits or inexpensive but extremely valuable computer security audits, so it's usually possible for a determined cracker to read, copy, alter or destroy data in well secured computers, albeit at the cost of great time and resources. Extremely few, if any, attackers would audit applications for vulnerabilities just to attack a single specific system. You can reduce a cracker's chances by keeping your systems up to date, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful backing up and insurance.

3.4 Security Measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes:

1. Prevention
2. Detection
3. Response

- User account access controls and cryptography can protect systems files and data, respectively.

- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.

- Intrusion Detection Systems (IDS's) are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored.

Today, computer security comprises mainly "preventive" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the Internet, and is normally implemented as software running on the machine, hooking into the network stack (or, in the case of most UNIX-based operating systems such as Linux, built into the operating system kernel) to provide real-time filtering and blocking. Another implementation is a so called physical firewall which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet (though not universal, as demonstrated by the large numbers of machines "cracked" by worms like the Code Red worm which would have been protected by a properly-configured firewall). However, relatively few organisations maintain computer systems with effective detection systems, and fewer still have organised response mechanisms in place.

3.5 Difficulty with Response

Responding forcefully to attempted security breaches (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons:

- Identifying attackers is difficult, as they are often in a different jurisdiction to the systems they attempt to breach, and operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymising procedures which make backtracking difficult and are often located in yet another jurisdiction. If they successfully breach security, they are often able to delete logs to cover their tracks.

- The sheer number of attempted attacks is so large that organisations cannot spend time pursuing each attacker (a typical home user with a permanent (eg, cable modem) connection will be attacked at least several times per day, so more attractive targets could be presumed to see many more). Note however, that most of the sheer bulk of these attacks is made by automated vulnerability scanners and computer worms.

- Law enforcement officers are often unfamiliar with information technology, and so lack the skills and interest in pursuing attackers. There are also budgetary constraints. It has been argued that the high cost of technology, such as DNA testing, and improved forensics mean less money for other kinds of law enforcement, so the overall rate of criminals not getting dealt with goes up as the cost of the technology increases.

4.0 CONCLUSION

The impact of computer threats and attacks on organizations has been enormous and on the increase, so also are the forms of attacks on information systems. This informs the need for organizations to accord information system security more priority. From the developer's perspectives, more efforts should be used to develop more robust and secure systems.

5.0 SUMMARY

- Most current real-world computer security efforts focus on external threats, and generally treat the computer system itself as a trusted system.

- Serious financial damage has been caused by computer security breaches, but reliably estimating costs is quite difficult.

- Individuals who have been infected with spyware or malware likely go through a costly and time-consuming process of having their computer cleaned.

- There are many similarities (yet many fundamental differences) between computer and physical security. Just like real-world security, the motivations for breaches of computer security vary between attackers, sometimes called hackers or crackers.

- A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them.

- Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information.

- Today, computer security comprises mainly "preventive" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network.

- Responding forcefully to attempted security breaches (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss 5 forms of security threats to information in an organization.
2. Discuss the term “Computer Firewall”.

7.0 REFERENCES/FURTHER READINGS

Anderson, Ross J. Security Engineering: A Guide to Building *Dependable Distributed Systems.*

Schneier, Bruce. Secrets & Lies: Digital Security in a Networked World.

Peikari, Cyrus; Anton Chuvakin. Security Warrior.

Koziol, Jack; David Litchfield. The Shellcoder's Handbook: *Discovering and Exploiting Security Holes.*

Stoll. Clifford. The Cuckoo's Egg: Tracking a Spy through the Maze of *Computer Espionage, an informal -- and easily approachable by* the non-specialist -- account of a real incident (and pattern) of computer insecurity.

Schell, Roger R. (1996). The Internet Rules but the Emperor Has No *Clothes ACSAC 1996.*

Caelli, William (2002). Relearning "Trusted Systems" in an Age of *NIIP: Lessons from the Past for the Future.*

Noel, Davis (2000). Cracked, story of a community network that was cracked and what was done to recover from it.

MODULE 3

UNIT 1 INFORMATION AND COMMUNICATION TECHNOLOGY AND THE SOCIETY

CONTENTS

1.0 INTRODUCTION

The Information Technology (IT) revolution is changing every area of our lives. At an ever-increasing rate it is reshaping our work, our, home and our leisure activities and it is transforming the economic and social structures of our land. Lying of the heart of this transformation are computer and telecommunications systems which are important components of IT.

The potential for good is enormous, for the relatively cheapness and availability of the technology not only creates material wealth by improving the efficiency of our business; it also provides each one of us with access to what is now our greatest resource: information. We can all enjoy equal access to information on the TV and Radio, and most people have easy access to other sources of information. Anyone can subscribe to and dial up on-line databases and gain up-to-date information on any aspect of the world we live in, as well as access a range of educational, financial, shopping leisure and other services.

The potential for evil is also great, for the same technology is able to provide those in authority with large amount of information on the

citizen and that large amount of information can be used to restrict people's freedom.

Our dependence on the technology can work in the authority's favour, for by controlling it they could censor the information that the people received and so control the mind.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- explain the extent to which information and communication technology has negatively affected the society at large
- identify the ways in which our privacy is impacted by technology
- identify the health hazards associated with our interaction with information and communication technology
- state how to deal with the health hazards from the gadgets of information and communication technology
- highlight the impact of information and communication technology on employer-employee relationships
- explain piracy, its impacts and how to avoid it, even in corporate organizations
- explain what a virus is and how to guard against it.

3.0 MAIN CONTENT

3.1 Invasion of Privacy

The ability of information technology apparatus to collect, organize and sort data about people, and for such data or information to be traded by individuals or organization has resulted in the invasion of individuals and organizations. Invasion of privacy is often carried out by organizations that collect and trade information about individuals.

Widespread use of computers and computerized databases makes privacy a much broader issue than it was in the past. People trail computerized data by using credit cards, cheques and medical insurance.

How Privacy is Invaded

Information technologies provide numerous opportunities to intrude on others.

1. **Mailing List: A mailing list is a commercial database that** contains names, addresses, telephone numbers and sometimes

data related to each person on the list. Through the mailing list people are sent unsolicited mails and many are bewildered by the amount of such mails. People receive such mails because their data stored in the mailing list match the criteria set by whoever is sending the mails. Perhaps the most common way to get on a mailing list is to subscribe to a magazine.

2. **Credit Histories: A credit history is a list of accounts held by** people to show if such people are seriously delinquent in payment. It is so because no company wants to lend money to, or open an account for people who don't pay their bills. So before a company opens an account for a client, it will probably check the prospective client's record. This is true of telephone companies, banks, credit card companies and even estate agents. There are companies who keep these databases about people and they get credit histories by buying account data of customers of other companies and selling them back whenever a company or individual needs someone's credit history. These companies work just like mailing list companies.

3. **Corporations and their Employees: Another threat to privacy** can occur between a company and its employees. With electronic communications systems such as electronic mail and voice mail, we have a media that is controlled by corporate content systems. The company has access to the content of communication, even if employees intend their messages to be private. If you write an electronic mail to a friend at work, some other employees might have access to your message.

3.2 Health and Safety

The interaction between employees and information technology (IT) gadgets has resulted in some health issues. Information systems can have impact on health because they are part of the job environment. The field of ergonomics which studies the physical relationship between people and their tools indicates that computer usage results in backache, wrist injury, strained eyes and stress.

Backache results from sitting on an uncomfortable chair all day long working on the computer. The seats are uncomfortable because the backrest, armrest and heights of the seat are not adjustable.

Repetitive Stress Injuring (RSI) is a group of ailment caused by continually using the body in ways it was not designed to work. The most common is the carpal tunnel syndrome (CTS) a wrist or hand injury caused by extended periods of keyboarding. When the tunnel

leading to the carpal becomes distorted, it pinches the nerve that runs through it and causes a great deal of pain and disability.

Eye injury results from staring at a computer screen for long periods. Many users have found their vision deteriorating as a result of prolonged computer use. Increase stress level has been reported as one of the consequences of information technology. Some managers believe that their stress level has increase due to information overload. They believe IT has contributed to this overload and that routine use of V-mail, e-mail, fax, PC has not been liberating at all.

Solutions to Ergonomic Disorders

1. **Backache: The following recommendations are made to reduce** backaches resulting from using uncomfortable chairs. Use chairs with:

• Adjustable height: The chair should be adjustable so that the highs are parallel to the floor and the feet are on the ground.
• Lower-back support: The chair should have an adjustable back that provides for support when seating at normal position.
• Arm rests: The chair should have an arm rest which provides an extra degree of comfort when the user is working at a keyboard for long periods.

2. **Carpal Tunnel Syndrome (CTS): To prevent CTS, the** following recommendations are necessary:

• Set the keyboard at a proper height, ideally the hands should be at the same level with the elbows or slightly lower, when they hover above the keyboard.
• A wrist support could be used and it is built into a keyboard or just placed in front of it. A wrist support allows for the relaxation of the arms so that only the finger will be used in typing.
• Use an ergonomic keyboard that allows the hands to rest in a more natural position. These keyboards are designed differently from the conventional flat keyboards.

3. **Eye Injury: Recommendations to prevent/ minimize eye injury** are as follows:

• Don’t stare at the screen for a long stretch of time. (Maintaining your focus at the same distance for long periods tends to distort the shape of your lens, so look away from your computer occasionally).

- Position the monitor between 2 and 2.25 feet from your eyes. That range is close enough to see everything on the screen but far enough to let the eyes take in the whole screen at once.
- Position the monitor in such a way that no light, including sunlight, reflects off the screen.
- Install an anti-glare screen to prevent reflection of light off the screen of the monitor.
- Use a monitor that holds steady image without pulsating or flittering.

4. Cell Phone Hazard

The Surgeon General warns that mobile phone handsets could be dangerous to health. Experts have warned that radioactive emission from cell phones is hazardous to human health.

Although there is still a dearth of research on the issue, medical experts say the energy emitted by cell phones, like all other devices that generate electromagnetic waves causes minimal local over heating of the brain. Based on this fact, they believe it will be wise to work on the scientific premise that cell phones, like every other device that generates electromagnetic waves should be handled with care.

Appliances such as television, monitor screen of computers, private mobile radios and cell phones are generally held to be capable of exposing humans and material equipment in their vicinity to radio frequency fields in measures that could compromise the safety of such equipment or persons. Cell phones are low-power radio devices that transmit and receive electromagnetic radiation at frequencies of about 1000Mhz, just below the electromagnetic spectrum.

What appears to be the first public awareness on the health hazard of cell phones emerged in the year, 2000 in the United States when a phone user sued a handset manufacturer for failing to warn him of the dangers of prolonged use of the cell phone. The victim had suffered brain tumor, a condition his personal physician attributed to his usage of the cell phone.

3.3 The Impact of Technology on Employees and Employment

The impact of technology on people and work is discussed as follows:

Autonomy and Power

Autonomy in a job is the degree of discretion individuals or groups have in planning, regulating and controlling their own work. Power is the ability to get other people to do things. Information system can cause increases or decreases in either ones.

Information system may increase autonomy whenever the individual can control the use of tools. For example, a data analysis system might permit totally independent analysis work by a manager who previously had to ask for assistance to analyze data. Likewise, professionals such as engineers and lawyers can use information systems to do work themselves that previously would require more collaboration and negotiation with others.

In contrast, many information systems are designed to reduce autonomy. The need for limited autonomy is widely accepted in transaction processing and records keeping, such as taking orders, are designed to assure that everyone involved in a repetitive process such as taking orders or producing paychecks, uses the same rules for processing the same data in the same format. If individuals could process transactions however they wanted to, tracking systems and accounting systems would quickly degenerate into chaos.

In other situations, a competition – driven and cost-cutting economy is leading to increased electronic surveillance especially where computerized systems are used continually as part of work.

Just as information systems can affect autonomy, they can also affect power by redistributing information, changing responsibilities; and shifting the balance of power in an organisation. Across the organizational spectrum, information systems have increased the power of people who operate largely on facts and technical competence and have reduced the ability of people to give orders based on the power of their position. The availability of information across business functions has made it easier to resolve conflicts based on facts rather than opinions and power.

Information systems have had an important impact in reducing the power of many middle managers. Higher level executives can often use the MIS directly to get some of the information they once received from middle managers; in addition they can use communication systems such as e-mail to bypass middle managers and go directly to the individuals who know the most about a particular situation or issue. Middle managers may see information system squeezing them from below and above.

Use of Valued Skills

Information systems may have either positive or negative effects on people's skills. As a simple example, consider what happens when you rely on a pocket calculator to do arithmetic. Although you usually get the right answer quickly, your ability to do arithmetic without the calculator deteriorates through disuse. The calculator has the positive effect of helping you calculate more quickly;; and the negative effect of allowing your skill to decline.

New Information systems have enhanced the skills in a wide range of jobs. Management Information Systems have provided information to managers that helps them learn how to manage, based on analyzing facts rather than just on intuition.

Introducing information systems has also had the opposite effect in some cases, especially when the systems automated the judgment and discretion in work. Such systems redefined jobs by placing the individual's autonomy and authority with computer enforced consistency and control. Now a less skilled person could do the same task, and previous skills had less value. Reducing the value of skills previously needed to do specific types of work is called de-skilling.

Tasks most susceptible to de-skilling call for repetition, endurance and speed, rather than flexibility, creativity, and judgment. Such tasks are highly structured and can be described in terms of procedures. In general they could involve processing data or could involve physical actions such as spray -painting a new car. In some specific cases, de-skilling has occurred with the partial automation of decision processes once thought of as requiring years of experience. For example, managers in insurance companies once believed it took five years to become a reasonably good group health underwriter. The mystery in training new underwriters disappeared when a new system automated standard underwriting calculations. Although the system's purpose was to provide better customer service and reduce the stress of year end peak loads, it also de-skilled the job. New underwriters could be productive on simple cases within months, and the knowledge of the more experienced underwriters was less valued.

Information systems may require that workers learn new skills. For professionals, the skills may involve new analytical tools or methods or new ways to obtain information.

Meaningfulness of Work

Information systems can affect the meaningfulness of work in several ways. First, the information system can be set up to either expand or limit the scope, variety and significance in the user's job. In addition the mere fact that work takes place through the medium of a computer, it may affect the way people experience the work.

1. **Variety and Scope of Work: Information systems can either** increase or decrease the variety and scope of work. Information systems reduce variety of work if they force the worker to focus on a small aspect of work. Consider what happened with the implementation of a computer- based dental claim system at an insurance company. With the previous paper–oriented system, the benefits analyst pulled information about each account from a set of paper files, checked contract limitations and completed the necessary paper work. With the new computerized system, much of the information was on the computer, which also ran programs that assured claims were processed in a standard way. The analyst spent more time entering claims data into computers and less time using their knowledge and judgment. With the computerized system the analysts were finding it difficult to retain information about their accounts, and complained of not being in control. within a year the system had increased productivity from 30% to 40%, but at the cost of job satisfaction for the analysts.

2. **The Nature of Computer-Mediated Work: The fact that work** is done through a computer may affect its meaningfulness to participants. Work done using computers, rather than through direct physical contact with the object of the task is called computer–mediated work. For example in a computer- mediated office work or record keeping, the worker uses a terminal to record and retrieve data instead of writing on paper. The work takes place through the computer, there is less reason to get up, walk over to a filling cabinet or even open a drawer. The computer becomes the only important physical contact.

Social Relationship

Social interaction at work is an important part of many people's lives that work systems can affect. In some cases computerized systems may create new possibilities for interaction by automating repetitive paperwork and calculations, thereby giving people more time to work on the issues that require interaction with others.

Furthermore, communication systems such as e-mail support additional contact between people separated geographically or organizationally.

Impacts of computerized systems on social relationships may also be negative, however. Jobs that require sitting at visual display terminals all day long tend to reduce social interaction. Trends toward downsizing and telecomm uniting amplify isolation and alienation because they reduce the number of people working in organizations and permit these people to work from home.

3.4 Computer Crimes

Computer and other associated information and communication technology equipment have formed the basis for improvement in business, governance, education, leisure and so on. On the other hand computer and telecommunications equipment have been abused resulting in crimes of different kinds. Discussed in this section are crimes that are associated with information technology apparatus.

1. Software Piracy

By far the biggest problem affecting the computer industry today is software piracy, which is illegal copying or use of programs. Piracy is such a big problem mainly because it is easy to carry out. In most cases, it is no more difficult to steal a program than it is to copy a CD that you have borrowed from friend, however both are illegal.

Part of the reason that piracy is so difficult to stop is that some kind of copying are legal, a fact that tempts people to gloss over the distinctions. For example, it is generally legal to copy software that you rightly own so you have a back up copy in case the original one is damaged. In fact installing a new piece of software means copying the program diskettes to your computer's hard disk and installation instructions usually advice users to make a back up copy on another set of diskettes.

Effects of Software Piracy

a. In the United States 25% of software in use are illegally copied and in 199 it cost the U.S economy $4.5 billion in lost wages, nearly $991 million in lost tax revenue and more than 109,000 lost jobs.

b. The costs to businesses and agencies using pirated software are :

- Higher cost of PC ownership. A PC system's total cost of ownership reflects all the costs of using the system; the purchase price, technical support, service and every thing else you need to the most from a PCs
- Lack of technical support
- Software incompatibility
- Viruses

• Legal costs and fines

c. Piracy puts the honest software reseller on an uneven playing field, often bidding against competitors who used illegal products as a price weapon. Unchecked, these practices destroy honorable businesses, handing over huge portion of the PC distribution channel to pirates.

Strategies to Protect Software Piracy

i. Copy Right Protection: Software companies make their programs with safeguards that prevent them from being copied, but that makes installation and back up difficult. For example, some program disks are set up such that they could be copied to the purchaser's hard disk only a few times. But most companies have found that this kind of copy protection causes more problems than it solves.

ii. Copy Right Law: Most companies today rely on the law and on people's respect for the law. The principal law governing software protection is the copyright of 1976 (USA). The justification for the law is that software is intellectual property, usually created with the intent of making money. The laws against software piracy were created to protect the interests of people and companies that develop software.

Without such legislation, creating good software might not be worth the investment and without good software the computer revolution would be over.

iii. Network Version and Site Licenses: Organizations that run a group of computers and want to run the same program on several of them are relatively common. Given the potential for loss of revenue caused by piracy, may software companies have adopted a strategy of selling site licenses and network versions of their programs. A site license is an agreement through which the purchaser of a program buys the right to use that program on a given number of machines for less than the price of buying a separate copy of the program for each computer.

Essentially the site licenses are a way for software companies to discourage piracy by offering a volume discount.

Network version is a variation of the site license. Today many companies connect all their computers in a local area network (LAN). A network version allow such companies buy just one copy that it can legally load onto its network and let some or all of its employer use.

iv. Shareware: Another strategy for combating software piracy is shareware, which is software that is distributed free on a trial basis. If a user decides to keep the program and continues to use it, the user is requested to pay the developer.

The shareware arrangement allows developers to load programs unto public information fora such as the Internet or electronic bulletin boards, making this software available to a broad group of customers without any sales or advertising costs.

The logic here is that since these programs are often more limited in scope or appeal than mainstream software, people are more likely to copy them illegally than to pay exorbitant fee to any such program.

v. Freeware: One final answer to the problem of software piracy is freeware. Such programs are free. Occasionally, people develop programs for their own use and then make them available to other people free. The most common place to find freeware is on electronics bulletin boards and information services such as the Internet. Usually freeware programs are not complex applications.

How to Guard against Piracy in Organizations

The following are some of the steps and actions to be taken to guard against piracy in an organization:

(i) Acquire software from only reputable dealers
(ii) Always keep the original disks: documentation and Certificate of Authenticity and End User License Agreement.
(iii) Appoint a software manager who should track software acquisition and conduct periodic audits at least yearly, keeping the software inventory in line with licenses and documentation.
(iv) Conduct software audit; first counting all PCs in your company and the software installed on them. The process includes having all the software product names, version numbers and serial numbers and scan PC hard disks.
(v) Conduct inventory of all documentation, including original disks, manuals, licenses, invoices and receipts. Discrepancies will usually reveal unlicensed software.
(vi) Announce a piracy prevention policy to keep your organization in line with the law.

2. Computer Viruses

Although software piracy is by for the most prevalent computer crime, an equally disturbing one is the creation of computer virus. A virus in the computer realm is a parasitic program buried within another legitimate program or stored in a special area called boot sector. Executing the legitimate program or accessing the disk activates the virus. Viruses can be programmed to do many things, including copy themselves to other programs, display information on the screen, destroy data files, or erase an entire hard disk. A virus can even be programmed to lie dormant for a specified time or until a given day.

Computer viruses do not occur naturally, each one must be programmed. There are no beneficial viruses. Sometimes they are written as a prank, perhaps to pick on people by displaying humorous messages. But when viruses are malicious and do real damage the real purpose is not known.

Types of Viruses: Among the numerous types of viruses known are Friday 13th, Alabama, Vienna, Christmas, Stoned (Marijuana), Pakistani, Brain, Opeyemi, Shankar, etc.

Preventing Infection: Fortunately, safeguarding a system against viruses is not that difficult, given a little knowledge and hard work. Once viruses are in computer memory, they destroy programs and data files on the hard drive.

The most common way to pick up a computer virus is by trading programs or disks with other people. Treat all disks as potential carriers of infection.

Checking for virus requires anti-virus software, which scan disks and programs for known viruses and eradicate them. Once a good anti-virus is installed on a system and activated, it checks for infected files automatically every time a diskette or modem is inserted or put to use.

Note that new viruses are constantly appearing so no program can offer absolute protection against all viruses.

4.0 CONCLUSION

In conclusion regardless of the true purpose of an information system, there is no way to guarantee the information in the system will be protected from someone intending to misuse it for an illegal or simply inappropriate purpose.

5.0 SUMMARY

This unit has highlighted the following pertinent points:

- The information and communication technology (IT) revolution is changing every area of our lives. At an ever-increasing rate it is reshaping our work, our, home and our leisure activities and it is transforming the economic and social structures of our land.

- The ability of information technology apparatus to collect, organize and sort data about people, and for such data or information to be traded by individuals or organization has resulted in the invasion of individuals and organization.

- The interaction between employees and information technology (IT) gadgets has resulted in some health issues. Information systems can have impact on health because they are part of the job environment.

- The Surgeon General warns that mobile phone handsets could be dangerous to health. Experts have warned that radioactive emission from cell phones is hazardous to human health.

- Introducing information systems has also had the opposite effect in some cases, especially when the system automated the judgment and discretion in work. Such system redefined jobs by placing the individual's autonomy and authority with computer-enforced consistency and control.

- Information systems can affect the meaningfulness of work in several ways.

- By far the biggest problem affecting the computer industry today is software piracy, which is illegal copying or use of programs.

- Although software piracy is by far the most prevalent computer crime, an equally disturbing one is the creation of computer virus.

- The most common way to pick up a computer virus is by trading programs or disks with other people. Treat all disks as potential carriers of infection.

6.0 TUTOR-MARKED ASSIGNMENT

1. Outline the steps you would adopt to forestall piracy in your organization

2. Briefly discuss the impacts of information technology on power and autonomy in the workplace.

7.0 REFERENCES/ FURTHER READINGS

French, C.S. (1993). Computer Studies. DP Publishing Ltd.

Norton, P. (1995). Introduction to Computers. Macmillan/McGraw-Hill.

UNIT 2 THE LAW AND COMPUTER INFORMATION SYSTEMS

CONTENTS

1.0 INTRODUCTION

Computer information systems present a whole slew of legal issues. Whenever a new form of communication emerges, there is a concern that along with legitimate users will come some abusers. Just as networked computer systems can be used for political debate, they can also be used as an outlet for defamation. How should they be treated? Who is liable? Is it the user who originally posted the defamation or the system the operator who controls and provides the forum?

Information communication technology is about the fastest growing sector in the world. However, the growth of electronic communication and data manipulation has not been matched by an equal growth in understanding on the part of legislatures, the judiciary, or the bar. Many decisions involving computers and computer networks are fundamentally flawed by a lack of understanding of the technology and how the intricacies of a particular legal field apply to the particular technology. In some cases decisions are made and legislation is passed with no regard or understanding of what impact there will be on the technology being affected by the legislation or court decision. Only with a proper understanding of both the law and the technology will electronic communications grow unimpeded by the archaic residue of the legal system.

2.0 OBJECTIVES

At the end of this unit you should be able to:

:

- identify the legal issues applicable to the use of information and communication technologies in governance, business and commerce
- identify the legal provisions to govern the impacts of these issues
- explain what copyright is

• explain how to guard against copyright abuses.

3.0 MAIN CONTENT

3.1 Obscene and Indecent Material

Computer information systems can contain obscene or indecent material in the form of text files, pictures, or sounds (such as the recording of an indecent or obscene text). The degree of liability that attaches depends on which legal analogy is applied to computer information systems. Differences in regulation based on medium are a result of differing First Amendment concerns.

1. Obscenity

The Court expressed the test for obscenity as whether:

(a) the average person, applying community standards would find that the work, taken as a whole, appeals to the prurient interest,
(b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and
(c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

2. Indecent Speech

Speech that is not considered obscene may qualify as indecent. Indecent language is that which "describes, in terms patently offensive as measured by community standards, sexual or excretory activities and organs". Furthermore, the restrictions the government may place on indecent speech are very limited, especially when indecent material is transmitted via a medium that requires affirmative steps to access the indecent material. This limitation on the ability to restrict access to indecent material has been explicitly applied to distribution of indecent material via the Internet.

While there may be a strong interest in keeping indecent material away from children, restrictions cannot be placed on this material so as to unduly burden adult access to this material. Because the Internet does not (yet) provide any mechanism for establishing the age of users who may gain access to indecent material, any legislation that limits access to indecent material to adults may provide too great a restriction on the right of adults to access this material via computer network.

3. Child Pornography

Another area of content regulated on computer information systems is child pornography. Section 2252 of title 18 of the United States Code forbids knowing foreign or interstate transportation or reception by any means including, for example, visual depictions of minors engaged in sexually explicit conduct that has been converted into a computer-readable form. The act of sending child-pornographic pictures via computer network to solicit sex has also been held sufficient justification for increasing a pedophile's sentence. Investigations into illegal child-pornography distribution via computer network have resulted in a number of convictions due to child pornography trafficking on America Online.

3.2 Computer Crime

Computer crime is an ever-present area of concern for operators of networked computer systems. Operators continuously find themselves needing to devote substantial resources to avoid falling victim to system-crackers and the like. The term "computer crime" covers a variety of offenses, including: unauthorized access to and use of computer resources, data theft, damaging stored data, engaging in service attacks, trafficking in stolen passwords, spreading computer viruses, and a number of other related offenses. All of these activities are often referred to as "hacking.

1. Computer Fraud

The first federal computer crime law in the United States of America, entitled the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, was passed in October of 1984. The Act made it a felony knowingly to access a computer without authorization, or in excess of authorization, in order to obtain classified United States defense or foreign relations information with the intent or reason to believe that such information would be used to harm the United States or to advantage a foreign nation.

Obtaining information via unauthorized access from the financial records of a financial institution or from a credit reporting agency's consumer file was also outlawed by the act. Accessing a computer to use, destroy, modify, or disclose information found in a computer system, as well as to prevent authorized use of any computer used for government business (if such a use would interfere with the government's use of the computer) were also made illegal.

The Computer Fraud and Abuse Act present a powerful weapon for SYSOPs whose computers have been violated by hackers.

2. Traditional Fraud Committed Via Computer Network

More traditional types of fraud may also be carried out via computer network. State and federal regulators in the United States have recently started taking an active role in cracking down on fraudulent schemes committed via the Internet and on on-line services. The Federal Trade Commission, for instance, has the authority to prevent unfair or deceptive trade practices through the Federal Trade Commission Act and other statutes the agency is charged with enforcing. Under the authority of these statutes, the Agency has taken action against everything from "run of the mill" pyramid scheme operators to bizarre scams involving software that, when downloaded and run, surreptitiously disconnects the user's computer from his or her Internet service provider, and reconnects the user's computer to a Moldovan exchange (that, in actuality, is really reaching a server in Canada, but the call incurs charges as if the user were calling a number in Moldova). In case anyone had much of a doubt, service providers who surreptitiously reroute telephone calls to foreign countries in order to receive kickbacks from long distance companies can be held liable for the accompanying deception.

Similarly, if someone offers a product on-line, and then does not deliver, that "merchant" may be held liable under state equivalents to the Federal Trade Commission Act. At least one court has held that existing state antifraud laws are "an excellent weapon in the soon-to-be-expected war on Internet fraud.

3. Unauthorized Use of Communications Services

One of the favorite targets of computer hackers is the telephone. Telephone systems are susceptible to computer hackers' illegal use. By breaking into the telephone company's computer, hackers can place free long distance calls to other computers, and can get lists of telephone credit card numbers. Trafficking of stolen credit card numbers and other kinds of telecommunications fraud costs long distance carriers over $1 billion annually. Distribution of fraudulently procured long distance codes is often accomplished over bulletin board systems or by publication in electronic journals put out by hackers over computer networks.

In addition to a variety of other statutes which may clearly provide a remedy against such unauthorized use, it is possible that some protection from hackers is to be found in section 1343 of the Wire Fraud Chapter of the U.S. Code. This section prohibits the use of wires, radio or television in order to fraudulently deprive a party of money or property.

4. Viruses

As pointed out in the introduction, computer viruses are increasingly of concern--both for operators of computer information systems, and for users of the systems.

What legal remedies are available for virus attacks? Distributing a virus affecting computers used substantially by the government or financial institutions is a federal crime under the Computer Fraud and Abuse Act of USA. If a virus also involves unauthorized access to an electronic communications system involving interstate commerce, the Electronic Communications Privacy Act of USA may come into play. SYSOPs must also worry about being liable to their users as a result of viruses that cause a disruption in service. Service outages caused by viruses or by shutdowns to prevent the spreading of viruses could result in a breach of contract when continual service is guaranteed. However, contract provisions could provide for excuse or deferral of obligation in the event of disruption of service by a virus.

Similarly, system operators are open to tort suits caused by negligent virus control.

[A SYSOP] might still be found liable on the ground that, in its role as operator of a computer system or network, it failed to use due care to prevent foreseeable damage, to warn of potential dangers, or to take reasonable steps to limit or control the damage once the dangers were realized.

The nature of "care" has not been defined by court or by statute. Still, it is likely that a court would find that a provider is liable for failure to take precautions against viruses when precautions are likely to be needed. SYSOPs are also likely to be held liable for not treating files they know are infected. Taking precautions against viruses would be likely to reduce the chances or degree of liability.

5. Protection from Hackers

System operators need to worry about damage caused by hackers as well as damage caused by viruses. While hackers are liable for the damage they cause, SYSOPs may find themselves on the receiving end of a tort suit for negligent failure to secure their computer information system. For a system operator to be found negligent there must first be a duty of care to the user who is injured by the hacker. There must then be a breach of that duty, i.e., the SYSOP must display conduct "which falls below the standard established by law for the protection of others

against unreasonable risk of harm. Simply put, the SYSOP must do what is generally expected of someone in his or her position in order to protect users from problems a normal user would expect to be protected against. Events that the SYSOP could not have prevented--or foreseen and planned for--will not result in liability. A SYSOP's duty "may be defined as a duty to select and implement security provisions, to monitor their effectiveness, and to maintain the provisions in accordance with changing security needs. SYSOPs should be aware of the type of information stored in their systems, what kind of security is needed for the services they provide, and which users are authorized to use what data and services. System operators also have a duty to explain to each user the extent of his or her authorization to use the computer information service.

The same analysis applies to operator-caused problems. If the system operator accidentally deletes data belonging to a user or negligently maintains the computer system, resulting in damage, he or she would be liable to the user to the same extent as he or she would be from hacker damage that occurred due to negligence.

3.3 Privacy of Electronic Documents

Privacy has been a concern of computer information system providers from the very beginning. With the speed, power, accessibility, and storage capacity provided by computers comes tremendous potential to infringe on people's privacy. It is imperative that users of services such as electronic mail understand how these services work. They must understand how private the users' communications really are, and who may have access to the users' "personal" e-mail. The same is true for stored computer files. Similarly, it is important that system operators be aware of what restrictions and requirements exist to maintain users' privacy expectations.

1. Pre-Electronic Communications Privacy Act of 1986 of the United States of America

The person must have a subjective expectation of privacy, and to be reasonable, it must be an expectation that society is willing to recognize as reasonable. For example, most people have a reasonable expectation that calls made from inside a closed telephone booth will be private. For computer users, although the system operator can read the user's e-mail, there may still be an expectation of privacy, especially on a "closed" system such as America Online or CompuServe, as opposed to an

Internet transmission. However, this, of course, does not mean that a user may have a right to expect that the recipient of a message on an on-line service will keep the contents of a message secret.

Statutory protection of the right to privacy was originally provided by the Federal Wiretap Statute. However, this statute affected only "wire communication," which was limited to "aural [voice] acquisition." Even if the Act did cover transmission, it still did not cover stored computer data. This does not result in significant or comprehensive protection of e-mail or stored data.

2. Electronic Communications Privacy Act of 1986 of United States of America

Prior to the passage of the Electronic Communications Privacy Act, communications between two persons were subject to widely disparate legal treatment depending on whether the message was carried by regular mail, electronic mail, an analog phone line, a cellular phone, or some other form of electronic communication system. This technology-dependent legal approach turned the Fourth Amendment's protection on its head. The Supreme Court had said that the Constitution protects people, not places, but the Wiretap Act did not adequately protect all personal communications; rather, it extended legal protection only to communications carried by some technologies

The Electronic Communications Privacy Act deals specifically with the interception and disclosure of interstate electronic communications. It works both to guarantee the privacy of e-mail and also to provide an outlet for prosecuting anyone who will not respect that privacy. The statute provides in part that "any person who (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication" shall be fined or imprisoned.

3. Access to Stored Communications

Section 2511 of the Electronic Communications Privacy Act concerns the interception of computer communications while section 2701 of the Act prohibits unlawful access to communications which are being stored on a computer. E-mail, voice mail, and even pager data are stored at some point during the transmission process. Section 2701 reads, in part, "whoever--(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby

obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be subject to fines and/or imprisonment. Like section 2511, section 2701 includes provisions prohibiting the divulgence of stored messages. Importantly, while section 2701 allows law enforcement agencies to gain access to stored communications; it also specifically allows the government to permit a system operator to first make backup copies of stored computer data, subject to a valid search warrant. Section 2701 enables electronic communications to be preserved for use outside of any government investigation.

4. Privacy Protection Act of 1980of United States of America

Computer systems also fall under the protection of the Privacy Protection Act of 1980. The Privacy Protection Act immunizes from law enforcement search and seizure any "work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate commerce.

3.4 Copyright Issues

1. The Basics of Copyrights

Text, pictures, sounds, software--all of these can be distributed via computer systems--and all can be copyrighted. Section 101 of the Copyright Act of USA allows protection of "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.

The element of fixation is important in the copyright statute; a work that is not fixed is not covered by the statute, and any possible protection must come from local common law. A number of controversial cases have held that reading copyrighted material into a computer's Random Access Memory (RAM) constitutes making a copy (or a fixation). These cases are controversial because a computer's RAM retains information only while the computer is turned on, and requires a constant "refreshing" of the stored information in order to avoid losing the data. Thus, the information stored in a computer's RAM is only temporarily fixed, at best.

However, a temporary fixation is all that is required by the Copyright Act for the purposes of finding that a copy has been made. These cases are also controversial because, while the Copyright Act explicitly allows

copies of computer programs to be made in the limited circumstance of making an archival copy of the program or a copy necessary to utilize the software (i.e. a RAM copy), this section only covers computer programs.

A computer program is defined in the Copyright Act as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result". Arguably data in raw form, such as e-mail and sound and picture files, does not meet the definition of a computer program, and thus may not even be copied into a computer's RAM as is necessary to utilize the data without risking a copyright infringement (unless such a copy fits under one of the exceptions such as the fair use provision). More likely, raw data is covered by an implied license that allows the work to be copied in naturally expected circumstances.

As mentioned, the Copyright Act gives an author the exclusive rights to make copies of his or her works, as well as create derivative works that includes copies in computer readable form. Thus, scanned pictures, digitized sounds, machine readable texts, and computer programs are all subject to an author's copyright. Any attempt to turn original material into one of these computer-readable forms without the author's permission (unless the copy falls under one of the exceptions in sections 107-120) is a violation of the author's copyright.

With decreasing costs of data storage, and increasing access to computer networks, comes an increase in the number of computer archives, such as FTP (file transfer protocol) sites and World Wide Web pages. These computer archives store various types of data which can be searched by the archive user. The archive site can be searched, and the information can be copied by anyone with sufficient access to the archive. The ease with which information can be accessed and duplicated has some profound copyright implications. I will use as an example a "lyric server" which is an archive that stores lyrics to songs by assorted artists.

In the case of a lyric server, if someone is sitting down with an album jacket and typing the lyrics into the computer for distribution in the archive, the translation of the lyrics from the album jacket to a computer text file constitutes a potentially unauthorized copy. Similarly, if someone else types in the file and a system operator then puts the file into the archive for distribution, the SYSOP has violated the author's right to make copies of his or her work.

Once the file is in the archive for distribution, there may be a copyright violation every time the information is copied. While the archive user may not be making an infringing copy by just viewing the file contained

in RAM, if the archive is publicly accessible, viewing some types of files may possibly constitute a public performance or display of the copyrighted work, the rights of which are also protected. Display rights, however (as well as performance rights), are an inelegant fit in this context. When a work is transferred, it generally must be acted upon to produce a display of the work. Although some types of distribution may make the immediate display of a work a seamless process, most distribution technologies do not produce a display as a necessary *incident of accessing the work.*

To infringe these display and performance rights, it should be necessary that the computer system makes the copyrighted work available in a manner such that the work is immediately shown, recited, rendered, or otherwise played directly to the user (as some types of bulletin board systems operate). To not require this immediate accessibility would be to confuse the right to distribute copies with the right to perform or display a work. By allowing the transmission of raw data, the system operator is making available a public place in which to copy, but not *display, the work. Without some activity beyond merely transmitting the* work in a raw data form, to hold a system operator liable for violating a display right would be analogous to holding a place--such as a library, a newsstand, or a waiting room, or any other place which has copyrighted works available to the public--liable for violating the copyright holder's display or performance rights.

The Information Infrastructure Task Force of the Commerce Department has proposed amending the copyright law to include a new "transmission right. However, such a new right would do nothing but weaken the distinction between making and transmitting a copy. "Transmitting" a copy still entails the creation of new copies, which, as discussed, is already an exclusive right reserved to the copyright holder.

2. Copyright and Strict Liability

There is no intent or knowledge requirement to find a violation of copyright. Copyright infringement as a strict liability offense--intent is only a factor in calculating damages. When a work is copied, even if the person making the copy does not know or have reason to know that the work is copyrighted, an infringement may still be found. Even subconscious copying has been held to be an infringement.

3. Fair Use On-Line

Whether the unauthorized distribution or archiving of a copyrighted work constitutes a violation of Section 106 of the Copyright Act is also determined by whether the copying falls under one of the Act's exceptions. The most important exception is the "fair use" provision.

Fair use was traditionally a means of promoting educational and critical uses. Fair use, then, is an exception to the general rule that the public's interest in a large body of intellectual products coincides with the author's interest in exclusive control of his work, and it is decided in each case as a matter of equity

The Fair use provision contains a list of uses that are presumed to be acceptable uses of copyrighted works. The list includes use for criticism, comment, news reporting, teaching, scholarship, or research. This list may provide some guidance as to what constitutes legal use for the user of a computer information system, but not for the provider of the archive. The archive user may be safe in copying song lyrics from the lyric server if he or she is using the lyrics for the purpose of commentary, for example, but the SYSOP who provides the service may not have the same defense.

If a use is not one of those listed in the statute, the determination as to whether the use is "fair" is made by employing a four-factor test. The four factors are:

(1) the purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
(2) the nature of the copyrighted work;
(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
(4) the effect of the use upon the potential market for or value of the copyrighted work.

Each factor is to be weighed with the others in light of the underlying purpose of awarding copyrights.

3.5 Trademark and Unfair Competition Issues

Along with copyright issues, trademark and unfair competition issues are growing concerns in the on-line world

Federal Trademark Law of USA provides that:

(a) Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false

designation of origin, false or misleading description of fact, or false or misleading representation of fact, which--

(1) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or

(2) in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

4.0 CONCLUSION

Now that the current regulatory environment of computer information systems has been discussed, we are left wondering how well the regulations function to control Cyberspace. Many people fear that the current law does not effectively protect the rights of voyagers through Cyberspace. This has given rise to groups such as Computer Professionals for Social.

5.0 SUMMARY

- Whenever a new communications medium develops, there is a risk that it will be used to deliver material which society frowns on, such as obscene or indecent data. Computer information systems allow the distribution of this material in the forms of text, picture, and sound.

- One major use for computer information systems is transferring files. Legal issues arise when these transfers contain copyrighted material. A harder question is who should be liable when data transfers constitute copyright infringement--the transmitter? The system operator of the machine through which the material passes? The recipient who may have initiated the transfer?

- A continual threat to computer users is the computer virus. Viruses can be distributed via computer information systems, both consciously and unconsciously. They can be put into a system by someone intending to cause harm, or they can be innocently transferred by a user who has an infected disk.

- Information privacy is another issue for users and operators of computer information systems. With society becoming increasingly

computerized, people need to be made aware of the extent to which their stored data and electronic software are secure. The Fourth Amendment to the United States Constitution reads:

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.

• Yet, how does this Amendment apply to Cyberspace? Cyberspace is a vague, ethereal place with no readily identifiable boundaries, where a "seizure" may not result in the loss of anything tangible and may not even be noticed.

• Furthermore, when activities do occur that violate the law, where does one seek redress? When a network such as the Internet is accessible worldwide, and thus difficult to identify from where objectionable material is originating, jurisdiction becomes a complex question.

• In all of these cases, questions arise as to who is liable. If systems operators (SYSOPs) are not made aware of the legal issues they may face in running a computer system, they may either fail to reduce or eliminate harm when it is within their power to do so, or they may unnecessarily restrict the services they provide out of fear of liability.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss computer crimes and their legal implications.
2. Briefly discuss the key legal infringements arising from the use of information and communication technologies.

7.0 REFERENCES/FURTHER READINGS

David, J. Loundy (1992). E-Law 4.

UNIT 3 PROGRAMS AND PROGRAM LANGUAGES

CONTENTS

1.0 INTRODUCTION

You can buy a computer program for almost any purpose you can imagine; besides, the main stream productivity and applications (spreadsheet, word processing desktop publishing and database management system) you will find more specialized programs for running medical diagnoses, insurance claims, bank management, legal management, etc. One wonders, who created them and for what purpose.
This leads us to the issue of programming, which is the science of writing programs (known as software) for the computer.

A program or software is a collection of electronic instructions that programmers write using programming languages, and that a computer's central processing unit (CPU) can interpret to carry out a specific task.
On the other hand program languages are the languages programmers use to write programs.

2.0 OBJECTIVES

At the end of this unit you should be able to:

• explain what a computer language is
• differentiate low-level language from high-level languages
• identify the different types of high-level languages
• define the different types of fourth generation languages.
• translate high-level languages
• differentiate object-oriented program from structured programming

3.0 MAIN CONTENT

3.1 The Language of the Computer

The internal programming language for a particular chip is called machine language and the only real computer language is machine language; but to most people machine language is completely unintelligible. Even very short and simple procedures can be pages of numbers that represent the commands and data the CPU works with directly.

Writing programs in machine language is very difficult. It is the language that the computer uses and understands. Programmers need an intermediary between themselves and the machines, and so to turn computers into useful machines. Programmers had to develop a computer programs that could translate instructions, which were easier for programmers to read, write and understand. (Computer language – the commands of its instruction set.) Of course, because there were no such tools to begin with, the first of these programs had to be painstakingly written the hard way – in machine language. Instructions presented to the computer must ultimately be expressed in machine language/ instructions since only the computer can execute machine language.

Ultimately, every program has to exist in machine language for the computer to use it. But for people to be able to write programs effectively, they need a higher level language – a language that elevates the process above the detailed quagmire of digits that makes up machine instruction.

3.2 Low- Level Language/Assembly Language

The term low- level language is a general term that applies to languages such as assembly language which is close to machine language.

Thus, Assembly language is a low-level language that uses program codes in place of the 'Os' and 'Is' of machine language. On the other hand, rather than a cumbersome series of 1s and 0s, assembly language uses easily recognized symbols called mnemonics to represent instructions. An assembler is a program that takes instructions that are meaningful to people and assembles them into machine languages. The language that an assembler takes as its input is called assembly.

By today's standards, assembly language is very much a low-level language because its command corresponds one to one with the instruction set of a CPU. In fact, there is not just one assembly language. Each type of CPU that has a unique instruction set has its own assembly language. When programmers write programs in assembly language, they use a text editor (a simple word processor that stores only ASCII Text) to create a source file. ASCII stands for America Standard Codes for Information Interchange Then they run the assembly program, passing it in the name of the text file containing the source code/file and the desired name of the executable program file it will produce. The assembler translates the source code line for line into machine code and creates the executable program file.

Programmers seldom write programs of any significant size in assembly language. Instead they use it to fine-tune important parts of programs written in a higher language. Assembly language remains important because it gives the programmer total control of the computer's CPU, and as a result produces compact, fast and efficient code.

3.3 High – Level Languages

Originally, a high-level language is any language that is easier to understand than machine language. But currently a high-level language is a language that is further removed from the machine code than is assembly language. High-level languages use more meaningful words and phrases and also provided the kind of facilities for altering program flow. Most computer programs are written in high-level languages.

Some of the most widely used high-level languages are as follows:

FORTRAN: FORTRAN which stands for Formula Translator was one of the first high-level languages and was specifically designed for mathematical and engineering programs. As one of the first high-level languages it enjoys immediate and widespread acceptance after its introduction in 1957. FORTRAN was enhanced and standardized in 1966 and again in 1977 and 1990. The current version is known as FORTRAN –90. John Backus developed it with a team of programmers from IBM.

Because of its almost exclusive focus on mathematical and engineering applications, FORTRAN has not been widely used with personal computers. Instead, FORTRAN remains a common language in mainframe systems especially those used for research and education.

COBOL: COBOL which stands for Common Business Oriented Language was developed in 1960 out of the need by US Government to solve the problem of incompatibilities among computer manufacturers. Partly because of government's backing, COBOL won a widespread acceptance as a standard language. Interestingly, this early high-level language has some of the most English-like statements of any computer language. Although this makes COBOL programs easy to read, it makes the writing of COBOL tedious because of all the extra verbiage.

PL/I: IBM introduced this program in 1964 as a single language that could be used for both business data processing and scientific calculations. It is extremely complicated because it incorporates and extends most of the capabilities of both FORTRAN and COBOL. PL/I did not replace COBOL because businesses were not convinced it was worth the expense to rewrite their existing COBOL programs.

BASIC: The BASIC language which stands for Beginners All –Purpose Symbolic Instruction Code was developed in 1964. It started largely as a tool to teach programming to students. BASIC is indeed an easy language for beginners to learn.

Because of its simplicity, BASIC is quite popular and is the first high level language to be implemented on personal computers. The BASIC language is available on virtually all IBM and compatible PCs and is then one of the most popular languages among amateur programmers. Larger and more powerful versions of BASIC are also available and are widely used by professional programmers and by software development companies.

Although BASIC is an extremely popular and widely used language in education and among amateur programmers, it is not necessarily viable to commercial applications mostly because it does not have a large pool of tools as other languages offer.

ADA: This language was developed by the department of defense in 1980 to try to standardize data processing for its weapons systems and to make programs more reusable to reduce programming costs. It is a structured program that encourages modular designs and facilities, testing and reducing codes.

PASCAL: PASCAL was developed in 1971 and was intended to overcome the limitations of other programming languages and to demonstrate a proper way to implement computer language. It is a highly structured program and as such is considered an excellent language for learning about structured programming.

Pascal's strong points are its impeccable type checking and its control – flow facilities. Lately Pascal has become popular for implementing object-oriented extensions. It still remains largely an educational program which is what it is designed for; it is not too good for commercial development.

C: C language is often regarded as a thoroughbred of programming and was developed in the 1970s. C is regarded as a highly portable language, because programs written with it could easily be ported to other computers equipped with a compiler. Programs written in C produce fast and efficient executable codes. C is also a powerful language that can make the computer do a lot of things. Because of its freedom C programming is extremely popular and is the most widely used language among professional software developers for commercial applications. However, it is not particularly easy to learn C language.

C++: C++ was developed in early 1980s and is an improvement on C language. C++ language brings object orientation to C. Object provides an entirely new way of looking at programs. Unlike other languages, the C++ does not flow from beginning to end. Like C, C++ is an extremely powerful and efficient language. But C++ is even more difficult to learn than C. C++ is difficult because as a superset of C, you have to learn everything about C and then learn about object – oriented programming and its implementations with C.

JAVA: This program was developed in 1995 as a general purpose, object-oriented, application-development language for producing programs that operate in a distributed environment involving many different platforms. Java programs execute within a "Java virtual machine" that can be controlled by a Web browser. Operating within this constrained environment means that Java programs are machine dependent and therefore generate the same results on any CPU that is using any particular Web page. It also leads to serious disadvantage, however because programs written in Java run much slower than comparable programs that are optimized for a particular CPU. Programmers knowledgeable in C++ can become productive quickly in Java because it contains 90% of the constructs in C++ and leaves out some of its more complex features. Java is used in Internet applications.

3.4 Fourth Generation Languages

Other than programming languages for teaching, third generation languages (High Level Languages)are basically tools for professional programmers. The high level of programming skills needed to use these languages for business applications makes their direct use by business professionals impractical. Using these programs is arduous and time consuming even for professional programmers. These factors encouraged the development of new ways to make programmers more productive and to permit nonprogrammers to do programming work.
By definition, Fourth Generation Languages (4GLs) are a loosely defined group of programming languages that makes languages less procedural than third generation languages. The term 4GLs is closely associated with query languages and report generators for retrieving data from databases, although 4GLs can also perform transactions using databases. Many 4GLs are subsets of larger products such as DBMS or integrated systems for designing and building business applications.

The benefits of 4GLs extend to both programmers and end users. Programmers need less time and efforts to specify the required processing. Writing the same reporting program in COBOL might take 10 times as long because of all the details that must be incorporated into

COBOL programs. End users benefit because 4GLs provide a way to obtain information without requiring the direct help of a programmer. The use of 4GLs for queries and report generation reduces the pressure on programmers to write reporting programs to support immediate information needs.

Although 4GLs have been adopted widely because of their advantages, they did not replace COBOL and other 3GLs for a variety of reasons. The existing investments in over 100 billion lines of COBOL code made rewriting all these programs an enormous task with a questionable payoff, especially because it would involve a major training effort in addition to the program revisions. The capabilities of 4GLs were also too limited for a great deal of new development because they could not handle complex formats and logic and because they did not address of the issues related to client-server computing.

The four generations of programming languages defines an important stream of developments, which makes programming less procedural and permits the user to be more concerned with the desired processing or outputs rather than the specific method used for performing the processing.

Structured Query Language (SQL): This is the language at the heart of every database management system (DBMS). It was developed in late 70's and early 80-'s by IBM to be the standard query language for databases. It is regarded as a 4th Generational Language (4GL).

It is similar to conventional programming languages discussed thus far, however it differs because it is specifically designed for communicating with databases. Specifically most, most programming languages are still procedural in nature, that is command tell the computer what to do – instruction-by-instruction, and step by step. However, an SQL statement is not really a command to computer but it is rather a description of some of the data contained in a database. SQL is non-procedural because it does give step-by-step commands to the computer or database. It describes data and sometimes instructs the database to do something with the data.

Some of the requests made by SQL in database are:

- Which field you want to work with
- The table it will work with
- The criteria for selecting record.

The major companies supporting SQL are Microsoft Access, Oracle, Informix, Ingres and Borland. However Paradox does not directly support SQL.

HYPERMEDIA: Hypermedia is a programming environment that allows non-programmer users to create custom applications. Hypermedia is an extension of an earlier technology known as hyper text which is used to create electronic books. With hypertext, an author can create links between parts of a book or document. Hypermedia brings the multimedia facilities of graphics, video and sound to hypertext as well as bringing language based on objects, icons and metaphors. This is mostly because a hypermedia application must have access to a hypermedia environment to be able to function. Hypermedia programs are not translated into machine code by a compiler and linker.

3.5 Translation of High-Level Languages

Programs written in high-level languages have to be translated into machine code/language. There are two common methods of translating high- level languages:

1. **Compiler: This translation involves translating the whole** program completely, and then executing the machine language version. Using the compiler method is more useful if the same program is to be used again and again, since the translation gets done only once. When using a compiler, two versions of the program is created. The first version called the source file/ program /code is the one written in the high –level language. The compiler takes in this source program and produces a translated version called the object program/ code. The object program then has to be loaded into memory and executed. Some compilers only translate the source program into a low-level language such as assembly language instead of translating the source program into machine code. Some further translation is then necessary in order for the program to be executed.

2. **Interpreter: This method involves translating and executing** each program in turn, which means the retranslating of instructions within loops. The interpreter method is more useful if the program is to be used once as this is straightforward.

3.6 Structured Programming

Structure has been the watchword in computer programming and has been consistent with the view of computer users. This means that computer program language is effectively planned, organized and

structured. Structured programming languages are functional in nature i.e. they are based on functions, subroutines that do something such as to display a message on the screen, get some keyboard input from a user, or perform some mathematical process.

A typical program can easily have hundreds of individual functions. In structured programming, data and functions are district. Functions perform their work and may or may not alter some of the data in the data pool while accomplishing their task.

For example, when a program runs, the CPU begins executing the statements of the program at its main entry point. Generally, the entry point is considered to be the first line (or statement) in the program/file/code, although in some languages the main entry point may be elsewhere, and it's identified by a keyword such as "main". After execution of the first statement, control passes on to the next statement and so on, until the statement has been executed.
Then the program ends.

3.7 Object Oriented Programming (OOP)

The 1990s saw the beginning in experiencing a "paradigm shift" in software development in terms of Object Oriented Programming, where concepts of program, data and file structures are integrated in the concepts of objects and their persistence.

Object oriented programming is a program assembly using pieces, or objects, that encapsulates information with instructions and combine complex steps into a single procedure. An object on the other hand is a self –contained unit defined within an object –oriented programming statement and contains both data and functions.

Programs that use object- oriented programming technique still have functions and subroutines and have structure in the sense that program statements must have precise and accurate grammar, or syntax. Object orientation is different in that it allows the programmer to think moderately – to break up a programming project into components. Object oriented programming does not necessarily offer new capabilities but provides an elegant new approach to programming. However, the programs are rugged, that is, much less susceptible to problems that plague programs written in a structured manner. For example, with a traditional program, it is common to fix a problem and to create another in the process. When you program with objects it is not easy to break a program.

The concepts of object –oriented programming can seem abstract at first, but the resulting benefits of using objects are many. Programs become simpler, programming becomes faster and the burden of program maintenance is lessened.

The first language to support specifically OOP methods was called Smalltalk that was developed in the 1970s. It took sometime before the object –oriented approach to programming to begin to catch on. In the mid 1980s, versions of existing languages began to appear with object-oriented features. New versions of C, Pascal and BASIC support object-oriented extensions and there is also hyper card. Today the premier object-oriented programme is C++.

Some of the unique features of the object oriented program are class and **privacy.**

Class: A class is the definition of an object. To implement an object in a program, you define a class with a sequence of statements in the program's source code/ program. A class definition is essentially a description of an object including its data items and functions descriptions.

Privacy: Another feature of object the oriented program is that data and functions can be declared private in the class definition. Being private means that the data members are shielded from access by any program statements other than those initiated by the class itself. In fact, by default all the components of a class are private. This privacy feature translates into safety and security of the data.

Derivation: In an object –oriented program, the programmer does not have to create a class definition for every object. Objects can be derived from other classes. They can be identical or derived with modification.

4.0 CONCLUSION

Different ways of writing programs have evolved over time. However, no program can be written without the eventual involvement of the original machine language that can only be understood by the computer. With growing needs in society and business, more computer languages are written.

5.0 SUMMARY

- A program or software is a collection of electronic instructions that programmers write using programming languages, and that a computer's central processing unit (CPU) can interpret to carry out a specific task.

- The term low- level language is a general term that applies to languages such as assembly language which is close to machine language.

- Originally, a high-level language is any language that is easier to understand than machine language. But currently a high-level language is a language that is further removed from the machine code than the assembly language.

- By definition, Fourth Generation Languages (4GLs) are a loosely defined group of programming languages that makes languages less procedural than third generation languages.

- Hypermedia is a programming environment that allows non-programmer users to create custom applications. Hypermedia is an extension of an earlier technology known as hyper text which is used to create electronic books.

- Programs written in high-level languages have to be translated into machine code/language. There are two common methods of translating high- level languages.

- Structure has been the watchword in computer programming and has been consistent with the view of computer users.

- Though there are diversities of programming languages designed to address various human endeavors, no program can be written without the involvement of the machine language. Machine language is the foundation for any meaningful wide-purpose program. The methods of writing programs are evolving with time and need of the society.
- The 1990s saw the beginning in experiencing a "paradigm shift" in software development in terms of object oriented programming, where concepts of program, data and file structures are integrated in the concepts of objects and their persistence.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss about 10 high-level computer languages.
2. Differentiate an Interpreter from a Compiler.

7.0 REFERENCES/FURTHER READINGS

French, C.S. (1993). Computer Studies. DP Publishing Ltd.

Norton, P (1995). Introduction to Computers. Macmillan/McGraw-Hill.

Ron, W. (1995). How Computer Works. Macmillan Computer Publishing.

UNIT 4 COUNTRY CASE STUDY: ICT IN ALLEVIATING POVERTY IN INDIA

CONTENTS

1.0 INTRODUCTION

The World Development Report 2000/01: Attacking Poverty identifies three priority areas for reducing poverty: increasing opportunity, enhancing empowerment, and improving security. Opportunity makes markets work for the poor and expands poor people's assets. Empowerment makes state institutions work better for poor people and removes social barriers. Security helps poor people manage risk (World Bank 2001). In the light of current experiences in rural India and elsewhere in the developing world, it is apparent that ICT -defined as the set of activities that facilitate the capturing, storage, processing, transmission and display of information by electronic means- can be utilized to support poverty reduction strategies.

The use of ICT applications can enhance poor people's opportunities by improving their access to markets, health, and education. Furthermore, ICT can empower the poor by expanding the use of services and reduce risks by widening access to micro finance.

2.0 OBJECTIVES

At the end of this unit you should be able to:

- explain real life cases of ICT in development of economies
- identify ways in which ICT can be used to improve the conditions of the poor
- identify some projects in India that ICT has empowered
- explain how low-cost assess can be achieved from lessons in India
- examine some lessons to help in undertaking a successful ICT project to alleviate poverty
- Explain how the rural poor in India access ICT.

3.0 MAIN CONTENT

3.1 ICT Projects for Poverty Reduction in Rural India

Although most of the rural poor in India are isolated from the information revolution, there are several examples in rural India where ICT is used to contribute to poverty reduction in the areas of opportunity, empowerment and security. The following case studies

highlight ICT applications that are attempting to realize the potential of ICT.

1. Opportunity

Improving Access to Basic Services: India Healthcare Delivery Project

ICT can improve health care delivery to the poor. Telemedicine can diminish the cost and hardship of long distance travel for medical attention and diagnosis, and e-mail and medical list-serves can deliver at minimal cost recent medical findings to health workers lacking research and technological facilities.

Furthermore, ICT has simplified medical data collection, record management, and paper filing [11]. Handheld computers or Personal Digital Assistants (PDAs), are allowing auxiliary nurse midwives (ANMs) participating in the InfoDev-sponsored India Healthcare Delivery project to reduce redundant paperwork and data entry, freeing up time for healthcare delivery to the poor.

ANMs shoulder most of the responsibility for healthcare delivery in vast and densely populated rural areas. Their duty is to administer immunization, offer advice on family planning, educate people on mother-child health programs, and collect data on the rural population's growth, birth, and immunization rates. Each ANM serves 5,000. 4 people, typically residing in different villages and hamlets, often located several kilometers apart. ANMs usually spend between 15 and 20 days per month on data collection and registration. PDAs are facilitating data collection and transmission, saving up to 40 percent of ANMs' work time. Redundant data entry prevalent in paper registers is eliminated and reports are generated automatically. These gains in efficiency multiply the impact and reach of limited resources, thus expanding access to basic services [7, 8, 14].

2. Empowerment

Improving Access to Government Services: Gyandoot

ICT can be used by government agencies to transform relations with citizens and businesses. In India, as in much of the developing world, it is not uncommon for rural villagers to travel long distances to government district headquarters in order to submit applications, meet officials, obtain copies of public records, or seek information regarding prevailing prices in commodity markets. This involves the loss of a day's income as well as the cost of transportation. Once at the government office, the relevant official, record, or information could be

unavailable, forcing repeated visits and additional expenses. In effect, government officials working with paper records enjoy a monopoly over information and records.

Information disclosure and the possibility of interacting with officials also build pressure for government accountability. The poor become empowered because they feel they are getting a service rather than a favour.

Since January 2000, Gyandoot -a government-owned computer network- has been making government more accessible to villagers in the poor and drought-prone Dhar district of Madhya Pradesh. Gyandoot attempts to reduce the time and money people spend trying to communicate with public officials and to provide immediate, transparent access to local government data and documentation.

For minimal fees, Intranet kiosks –or telekiosks– provide caste, income, and domicile certificates, avoiding villagers the common practice of paying bribes. The telekiosks also allow farmers to track crop prices in the region's wholesale markets-enabling them to negotiate better terms. Other services include information on school results and on the names of people included in the below poverty line list, and a public complaint line for reporting broken irrigation pumps, unfair prices, absentee teachers, and other problems. Telekiosks are run by local operators along commercial lines and are placed in villages located on major roads or holding weekly markets, so that each of them can serve another 25 to 30 villages [6, 9].

3. Security

Improving access to microfinance: Smart Cards

Microfinance is an important tool for poor people to reduce, mitigate and cope with risk.Computerization, Smart Cards, and software systems providing loan tracking, financial projections and branch management information can reduce costs and help microfinance institutions reach clients more efficiently.

Smart Cards with an embedded microchip containing information on clients' credit histories are helping SKS, a microfinance institution operating in the Medak district of Andhra Pradesh to reduce transaction costs. One of the main problems faced by SKS, which follows the peer-lending model developed by the Best and Maclay [5] different telekiosks –which typically have only a single computer and are staffed with a facilitator– and telecenters –which have one or more

differentiate

personal computers and some access to the international telecommunications network.

Grameen Bank is the high cost of service delivery to the poor. All cash transactions take place at village group meetings and each transaction takes about 90 seconds per person. Much time is spent not only on paperwork but also discussing terms and conditions and counting coins. Office computerization alone would not bring much time savings because staff would have more free time during the day, but not in the mornings and evenings when people in villages are available for meetings.

Smart Cards have been identified as a solution to the high cost of delivery, because they can lead to gains in efficiency, eliminating paperwork, reducing errors, fraud and meeting time. Potential savings in operations are estimated to be around 18 percent. Once all of SKS operations are conducted with handheld computers, a read-only device will be left in each village for clients to check the information stored on the Smart Cards. Micro finance projects like SKS enable poor people and their micro businesses to gain broader access to financial services[1, 3, 8].

3.2 Access to ICT in Rural India

Of course, in practice the rich are likely to use both mobile phones and the Internet, but each for different purposes. Furthermore, mobile phones can in certain circumstances provide access to the Internet.

In India, even where telephone lines have reached rural areas through the introduction of Public Call Offices (PCOs), the poor have indeed very limited access to ICT. As revealed by a recent survey conducted in five villages in Uttar Pradesh, West Bengal and Andhra Pradesh [19], only radios are owned by a majority of poor households. Televisions, telephones and newspapers are available to the majority of households on a shared basis. Very few families have shared access to a computer or Internet connection, and some households have never viewed television, read a newspaper or used a telephone. Surveys also suggest that the poor rely on information from informal networks of trusted family, friends and local leaders, but these networks do not adequately satisfy their information needs [19]. This indicates that ICT could play a pivotal role in improving access to information by the poor. However, it remains very difficult for people with low levels of education to reap the full benefits of new technologies, including wide access to knowledge and information.

3.3 Achieving low-Cost Connectivity: A Necessary Condition for Pro -Poor ICT

While many factors contribute to the success of ICT projects in rural areas of developing countries, low cost access to information infrastructure is the basic necessary -but insufficient- condition to reach the poor. Inadequate or absent connectivity and unstable power supply clearly reduce the economic viability of ICT projects (Kirkman 1999). Gyandoot, for instance, faces problems with dial-up connections because most of the local rural telephone exchanges do not operate with optical fiber cable [6].Given that it is not realistic to provide telephone lines or computers to all households in developing countries, government and regulators should be concerned with policy instruments for achieving "universal access." The latter is generally defined as the presence of a public telecom booth in every village, or within reasonable distance [16, 18]. India is striving to achieve universal access through its national telecom policies focused on the provision of telecom facilities to every village at "affordable and reasonable prices" but almost 40 percent of rural communities still lack shared access to a telephone [22].

1. Fostering Competition

Fostering competition in the telecom sector can significantly reduce communication costs, and thus improve physical access to ICT by the poor. In countries that reformed their telecommunications sector, teledensity -the number of telephone mainlines per 1,000 people- grew at a much higher rate between 1996 and 2000 than in countries where reform had not taken place [4].

In India, teledensity has significantly improved between 1997 and 2000. This has been mainly the result of market-oriented reforms in the telecom sector. Prior to 1992, the Department of Telecommunications was the sole provider of telecom services in India, and the rigid regulatory framework was a big obstacle to the development of telecom infrastructure. In 1992, the mobile market was privatized. In 1994, the fixed services market followed and finally, in 1999, national long distance operations were opened to private competition [12].. Privatization permitted prospective telecom operators to bid for the right to operate in a whole state. Given the size of states in India, bids of over US$1 billion were common [17].

2. A Role for Small Entrepreneurs

Large telecom operators tend to limit their operations to higher-income urban areas because of the lower revenue potential of poor rural areas and the higher cost of servicing them. Small entrepreneurs, on the other

hand, see the opportunity to make a profit even in a lower revenue environment, and thus have the proper incentive to enter rural markets.
A good example of this is cable TV in India. Typically, micro entrepreneurs install dish antennas for cable TV and provide service to subscribers within a 700-meters radius. Operators sell the connection and visit homes to collect charges -between US$1.50 and US$4 per month. Customers know the operator personally, and the service operator is available to rectify problems anytime of the week. For these reasons, cable services in India are considered superior to telephone services, although cable technology is significantly more complicated than telephone technology. Consequently, it can be argued that privatization should be opened up to allow small entrepreneurs –or Local Service Providers- to supply telecom services in rural areas [17].

3. Regulatory Mechanisms

However, the market by itself might not be able to provide a sufficient level of connectivity to the poorest and most isolated rural areas. The key to achieving connectivity for these areas is to determine how far market forces will carry the rollout of voice and data networks. The gaps left by the private sector can then be remedied by public intervention. Regulatory mechanisms that can help extend access to information infrastructure include geographic coverage requirements and universal access funds.

One alternative is to invite private operators to bid for services in areas that are not commercially viable in return for a subsidy financed from a universal access fund. A concession contract is then awarded to the company requesting the smallest subsidy. In Chile, for example, this mechanism has been used to leverage US$40 million in private investment on the basis of just over US$2 million of public subsidy. As a result 1,000 public telephones have been installed in rural towns, at around 10 per cent of the costs of direct public provision. Subsidies of this kind could also be used to support the development of Internet-enabled community centers, content relevant to low-income groups and to people that speak languages not well represented on the web, and community postal and radio facilities [23].

3.4 Project Design Lessons

Even if information infrastructure reaches rural areas, there is no guarantee that the poor will access ICT applications. Many of the projects that attempt to provide access to the Internet in rural India, for instance, end up favoring middle and upper-class men [9, 10]. Rural women tend to be excluded because of their restricted mobility, lack of

education, and, in some cases, male control over information and media [2]. How can we ensure that ICT projects reach poor women and men?

1. Grassroots Intermediaries

In rural India, as in much of the developing world, direct ownership and use of ICT -for instance through a PC with Internet access- applies only to a very minimal fraction of the population. Although the availability of content in local languages and the use of graphic and voice interfaces can make ICT applications more accessible to poor people, illiteracy, low levels of education, gender, class and caste inequalities are powerful obstacles to the use of computers and other ICT tools.

It follows that, in most cases, poor people have to rely on a human intermediary between them and ICT, in what is termed a "reintermediation model" [14]. The profile of the intermediaries who add human skills and knowledge to the presence of ICT is thus critical for projects that want to reach the poor [13]. Successful examples of ICT projects for poverty reduction are conducted by intermediaries that have the appropriate incentives and proven track record working with poor people. If these intermediaries are grassroots-based and understand the potential of ICT for social change, they can be effective in promoting local ownership of ICT projects. In rural India, many telekiosks operators are young, educated, computer-savvy, and much attached to their communities. They are also extremely entrepreneurial. Given the right incentives and opportunities, these grassroots intermediaries are keen to make access to information easily available for everybody and are willing to train others in the villages [8, 9, and 10].

2. Community Involvement

Applications developed by or with the collaboration of local staff are more likely to be appropriate for local conditions when there is continuous involvement and feedback from the community. Local ownership fosters the success and resilience of ICT projects. Outside control and top-down approaches, on the other hand, often waste resources in the initial periods of projects endangering their sustainability.

In the case of e-governance projects, the local administrative and political machinery needs to be involved in the implementation of the project, or otherwise the chance of failure is almost certain. Information technology officers working on the CARD (Computer Aided Registration Department) e-governance project in Andhra Pradesh have also learned that it is important to develop constituencies outside the

political and administrative system, i.e. with citizens themselves. In Rajasthan, the state-sponsored RajNidhi e-governance program has failed to deliver, despite the fact that the software is easy to use and in Hindi, because of extremely centralized planning that did not take local conditions into consideration. Content, in fact, lacks regular updating because of communicationsproblems between the state and the local government [21].

3. Information Needs, Locally-Contextualized Information and Pro-Poor Services

Local, governmental, non-governmental and international organizations planning ICT projects in the field should thoroughly assess the information needs of a community before launching ICT projects. Rapid, participatory rural appraisals and other survey instruments have been used for several years to ensure community ownership of development programs. These tools could be used in the context of ICT initiatives [20].

Content provided through ICT should not be limited to the knowledge that can be accessed from outside sources, but rather extended to ensure that the poor have the means to speak for themselves. The poor know a great deal: they know their needs, circumstances, worries and aspirations better than anybody. The Honey Bee Network, with its database of solutions to local development problems, is an excellent example of the creation of relevant content for the lives of poor people [11]. It is advisable that ICT projects focus on a limited number of well-run pro-poor services –and expand them incrementally- rather than offer a great number of services that end up lying unutilized because of lack of demand.

4. Awareness-Raising and Training

Raising awareness among the poor about the potential of ICT is another important aspect of successful ICT projects. In the Dhar district of Madhya Pradesh, poor people are generally not aware of the services offered by Gyandoot. Although some efforts have been undertaken to raise awareness –by designing posters with pictorial depictions of the services offered at the telekiosks and by displaying prominent Gyandoot signs outside the telekiosks– more could be done [9]. Word of mouth is often a very powerful tool for publicity. The leaders of poor communities, as well as school children, could be brought to the telekiosks for a demonstration showing what ICT can do for them. Furthermore, the provision of content that is not directly related to development goals, such as news, matrimonials and entertainment information could also be a winning strategy to raise awareness about

telekiosks. A recent survey from rural India found that entertainment programs, together with news, are the types of information most frequently accessed by the rural poor. [19]. Training poor women and men in information technology skills is also important.

5. Financial Sustainability, Monitoring and Evaluation

Finally, a major challenge for ICT projects is reaching financial sustainability. Connectivity can be particularly expensive. In urban areas of India, each fixed-line telephone connection costs more than US$650. A phone booth operator needs to earn at least US$190 per year to break even. Telephones in rural areas are even dearer - a line can cost US$1,500-1,700. To break even, the annual revenue per line would have to be around US$425 [21]. Since most ICT projects are recent and not expected to reach self-sustainability for three or four years, experience on sustainability is limited. Gyandoot, which started operating in 2000, has seen few telekiosks reach commercial viability.

How will we know whether the benefits derived from ICT projects outweigh the costs? In order to answer this and other questions, rigorous monitoring and evaluation (M&E) of the social and economic benefits of ICT projects in rural areas are needed. M&E measure performance, identify and correct potential problems early on, and improve the understanding of the relationship between different poverty outcomes and ICT policies [18]. M&E are especially needed to measure the success of many pilots currently under way. In fact, in the case of pilots, successful outcomes might be implicitly biased due to the choice of favorable places and conditions. Projects might not yield the same results in more challenging and realistic situations.

4.0 CONCLUSION

Reaching the poor and realizing the potential of ICT for poverty reduction in the areas of opportunity, empowerment and security is a difficult endeavor. Nevertheless, ICT projects implemented by grassroots - based organizations and individuals who have the appropriate incentives to work with marginalized groups can achieve encouraging results. Successful ICT projects are characterized by local ownership and the participation of the community.

5.0 SUMMARY

- The use of ICT applications can enhance poor people's opportunities by improving their access to markets, health, and education. Furthermore, ICT can empower the poor by expanding the use of

government services, and reduce risks by widening access to micro finance.

• ICT has simplified medical data collection, record management, and paper filing [13]. Handheld computers, or Personal Digital Assistants (PDAs), are allowing auxiliary nurse midwives (ANMs) participating in the InfoDev-sponsored India Healthcare Delivery project.

• Since January 2000, Gyandoot -a government-owned computer network- has been making government more accessible to villagers in the poor and drought-prone Dhar district of Madhya Pradesh. Gyandoot attempts to reduce the time and money people spend trying to communicate with public officials and to provide immediate, transparent access to local government data and documentation.

• Microfinance is an important tool for poor people to reduce, mitigate and cope with risk. Computerization, Smart Cards, and software systems providing loan tracking, financial projections and branch management information can reduce costs and help microfinance institutions reach clients more efficiently.

• In India, even where telephone lines have reached rural areas through the introduction of Public Call Offices (PCOs), the poor have indeed very limited access to ICT.

• While many factors contribute to the success of ICT projects in rural areas of developing countries, low cost access to information infrastructure is the basic necessary -but insufficient- condition to reach the poor.

• In India, teledensity has significantly improved between 1997 and 2000. This has been mainly the result of market-oriented reforms in the telecom sector.

• A recent survey from rural India found that entertainment programs, together with news, are the types of information most frequently accessed by the rural poor. Training poor women and men in information technology skills is also important.

• Finally, a major challenge for ICT projects is reaching financial sustainability. Connectivity can be particularly expensive.

6.0 TUTOR-MARKED ASSIGNMENT

1. Identify and discuss the factors that bring about poverty reduction using ICT.
2. Identify and briefly discuss three projects in rural India powered by ICT.

7.0 REFERENCES/FURTHER READINGS

Akula, V. B. (2000). "Putting Technology to Work for Poverty Alleviation": A Draft Proposal for $151,030 to Develop Smart Cards for Microfinance. Hyderabad: Swayam Krishi Sangam.

Balit, S. (1999). Voices for Change: Rural Women and Communication. Rome: FAO.

Baramati Initiatives (2001). "SKS-Smart Cards: A Case Study".

Beardsley, S; Beyer, I. von Morgenstern; Enriquez, L & Kipping, C (2002). "Telecommunications Sector Reform –A Prerequisite for Networked Readiness" in The Global Information Technology *Report 2001-2002: Readiness for the Networked World. Oxford* University Press.

Best, M. L and Maclay C.M (2002). "Community Internet Access in Rural Areas: Solving the Economic Sustainability Puzzle" in The *Global Information Technology Report 2001-2002: Readiness for the Networked World. Oxford University Press, 2002.*

Bhatnagar, S. &Vyas, N. (2001). Gyandoot: Community-Owned Rural *Internet Kiosks., Washington D.C.*

Bhatnagar, S. and Schware, R.(eds.) (2001). Information and *Communication Technology in Rural Development: Case Studies from India. World Bank Institute Working Papers, 2000.*

Cecchini, S. (2001). "Back to Office Report: Information and Communications Technology for Poverty Reduction in Rural India," Washington D.C: Mimeo, World Bank.

Cecchini, S (2002). "Back to Office Report: Evaluation of Gyandoot and Bhoomi and International Conferences on ICT for Development," Washington D.C: Mimeo, World Bank.

Cecchini, S and Raina, M (2002) "Warana: The Case of an Indian Rural Community Adopting Information and Communications

Technology" in Information Technology in Developing *Countries, Volume 12, No. 1, April 2002.*

Cecchini, S and Shah, T (2002). "Information and Communications Technology as a Tool for Empowerment" in Empowerment and *Poverty Reduction: A Sourcebook. Washington D.C: World* Bank.

Digital Opportunity Initiative,(2001). "Creating a Development Dynamic: Final Report of the Digital Opportunity Initiative".

Heeks, R (1999) "Information and Communication Technologies, Poverty and Development," Development Informatics Working *Paper Series, Paper No. 5, 1999.*

Heeks, R (2001) "Understanding e-Governance for Development." i-*Government Working Paper Series, Paper No. 11, 2001*.

InfoDev, InfoDev Quarterly Report. Washington D.C: World Bank (various years).

James, J (2000) "Pro -Poor Modes of Technical Integration into the Global Economy" in Development and Change. Vol. 31, 2000, 765-783.

Jhunjhunwala,A (2000) "Unleashing Telecom and Internet in India," Paper presented at India Telecom Conference at the Asia/Pacific Research Center, Stanford University, November 2000.

Kenny, C J; Navas-Sabater & Quiang, C (2001) "Information and Communication Technologies and Poverty" in World Bank *Poverty Reduction Strategies Sourcebook, 2001*.

Pigato, M (2001). "Information and Communication Technology, Poverty and Development in sub-Saharan Africa and South Asia," World Bank: Washington D.C.

Richardson, D and Paisley, L (1998) eds. The First Mile of *Connectivity, FAO, Rome, 1998.*

Syngh Yadav, K.P. (2001). "Virtually There" in Centre for Science and Environment, Down to Earth Magazine, Vol. 9, No. 18, February 2001.

Telecom Regulatory Authority of India, Recommendations of the TRAI on "Universal Service Obligation," 2001.

World Bank, Information and Communication Technologies: A World *Bank Group Strategy, Washington D.C.*