COURSE CODE: **COM 112**

COURSE TITLE: **COMPUTER OPERATIONS**

COURSE UNIT: **2**

OUTLINE

1. Organisational structure of a data processing department
2. Computer Operations procedure
3. Data preparation procedure
4. Computer security
5. Computer file structure

UNIT 1: **ORGANISATIONAL STRUCTURE OF A DATA PROCESSING DEPARTMENT**

1.0 Introduction

Most ICT firm, organization and institution will most likely have a data processing department. The core function of a data processing department or data management centre is to process data. The structure of this unit in the organization is being organized in such a way that a skilled professional personnel is put in place to oversee the administration of the centre who in turn reports to the executives or the directors board on the necessary protocols needed in putting the data processing department in such a way that it would be in line with the organization or institution objective.

The size of the data processing department of an organization and the degree of separation of functions within it depend on the size of the organization and the extent of computerization within it. Another factor that determined the size of an organization's data processing department is the financial considerations.

Before we discuss the organizational structure of a functional data processing department or data management centre, let deals with some fundamentals of the processes that are being carried out at this centre.

1.1 Data processing

Data are a collection of facts — unorganized but able to be organized into useful information. Processing is a series of actions or operations that convert inputs into outputs. When we speak of data processing, the input is data, and the output is useful information. What then is data processing? So, we can define *data processing* as a series of actions or operations that converts data into useful information.

According to Carl (1996) data processing is, broadly, "the collection and manipulation of items of data to produce meaningful information. In this sense it can be considered a subset of *information processing*, "the change (processing) of information in any manner detectable by an observer. The term is often used more specifically in the context of a business or other organization to refer to the class of commercial data processing applications.

Also by Illingworth (1997), the term Data processing (DP) has also been used previously to refer to a department within an organization responsible for the operation of data processing applications. This processing evolves from manual to electronics as it can be seen today by the use of computer to process data faster and more efficiently.
Data processing (numerical and non-numerical) includes the analysis of various, sorting, calculating, editing, processing and handling data. The increasing popularity of computers in the field of computer applications, a small proportion of numerical calculation by computer data processing for information management has become a major application. Such as the side of the draw chart management, warehouse management, accounting management, transportation management, IT management, office automation. Geographical data in a large number of existing data in the natural environment (land, water, climate, biological and other resource data), there are a large number of socio-economic data (population, transport, industry and agriculture, etc.), often require comprehensive data processing. Therefore, the need to establish geographic database, the system to collate and store geographic data to reduce redundancy, the development of data processing software, full use of database technology for data management and processing.

Data processing system includes the resources that are used to accomplish the processing of data. There are four types of these resources:

- people
- materials
- facilities and
- equipment

People provide input to computers, operate them, and use their output. Materials, such as paper and printer cartridge, are consumed in great quantity. Facilities are required to house the computer equipment, people and materials.

1.2 Data processing functions

Data processing may involve various processes, including:

- Validation – ensuring that supplied data is clean, correct and useful.
- Sorting – arranges items in some sequence and/or in different sets.
- Summarization – reduces detail data to its main points.
- Aggregation – combines multiple pieces of data.
- Analysis – involves collection, organization, analysis, interpretation and presentation of data.
- Reporting –lists detail or summary data or computed information.
- Classification – separates data into various categories.

Each of these processes culminates into what the personnel in a data processing department carried out daily.

There are five basic operations that characterize all data processing systems:

- inputting
- storing
- processing
- outputting and
- controlling

Inputting is the process of entering data, which are collected facts, into a data processing system. *Storing* is saving data or information so that they are available for initial or for additional processing. *Processing* represents performing arithmetic or logical operations on data in order to convert them into useful information. *Outputting* is the process of producing useful information, such as a printed report or visual display. *Controlling* is directing the manner and sequence in which all of the above operations are performed.

Processing data using computer system has been seen as a better option to the obsolete manual methods of data processing. Thus, all organization mostly use computer to process data in their various data processing department. Some of the advantages of using computer for data processing are highlighted below:

i. **Accuracy**: once data have been entered correctly into the computer component of a data processing system, the need for further manipulation by humans is eliminated, and the possibility of error is reduced. Computers, when properly programmed, are also unlikely to make computational errors. Of course, computer systems remain vulnerable to the entry by humans of invalid data.

ii. **Ease of communications**: Data, once entered, can be transmitted wherever needed by communications networks. These may be either earth or satellite-based systems.

iii. **Storage capacity:** Computers are able to store vast amounts of information, to organize it, and to retrieve it in ways that are far beyond the capabilities of humans. The amount of data that can be stored on devices such as magnetic discs (HDD) is constantly increasing. All the while, the cost per character of data stored is decreasing.

iv. **Speed**: The speed, at which computer data processing systems can respond, adds to their value. The response required might be a fraction of a second. Thus, an important objective in the design of computer data processing systems is to allow computers to do what they do best and to free humans from routine, error prone tasks.

The most cost-effective computer data processing system is the one that does the job effectively and at the least cost. By using computers in a cost-effective manner, we will be better able to respond to the challenges and opportunities of our post-industrial, information-dependent society.

2.0 Personnel in a Data Processing Department

In the department various staff with different computer skills is being employed. The data processing manager is the head of the department under which we have the computer analyst, programmer, operation manager, etc. There is probably no standard structure for

data processing department. Precise responsibilities and reporting procedures vary. Figure 1 and 2 below show an example.

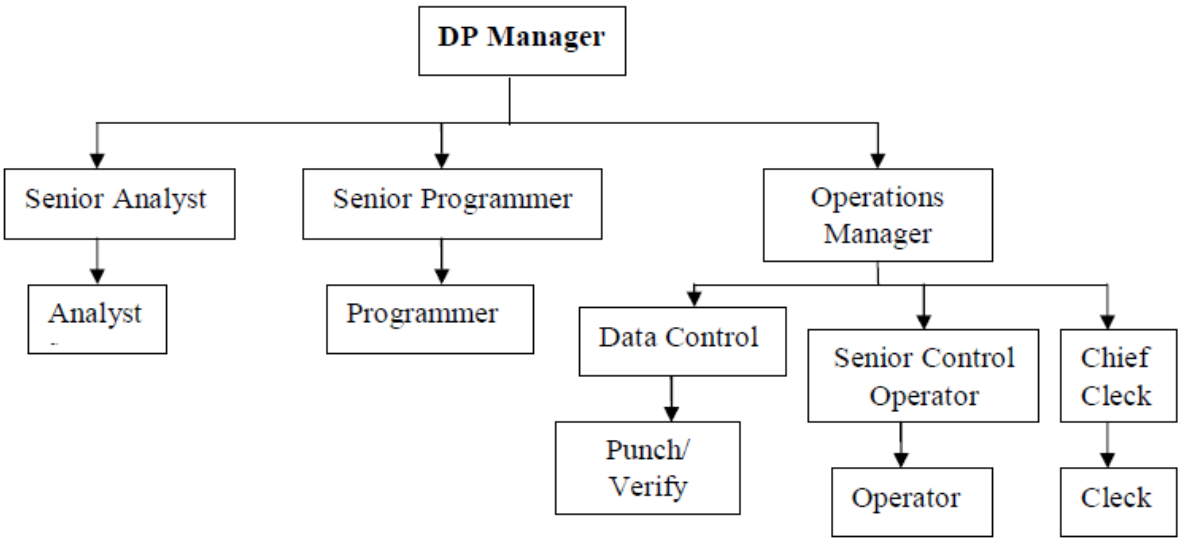

Fig. 1. Data Processing Department Structure I

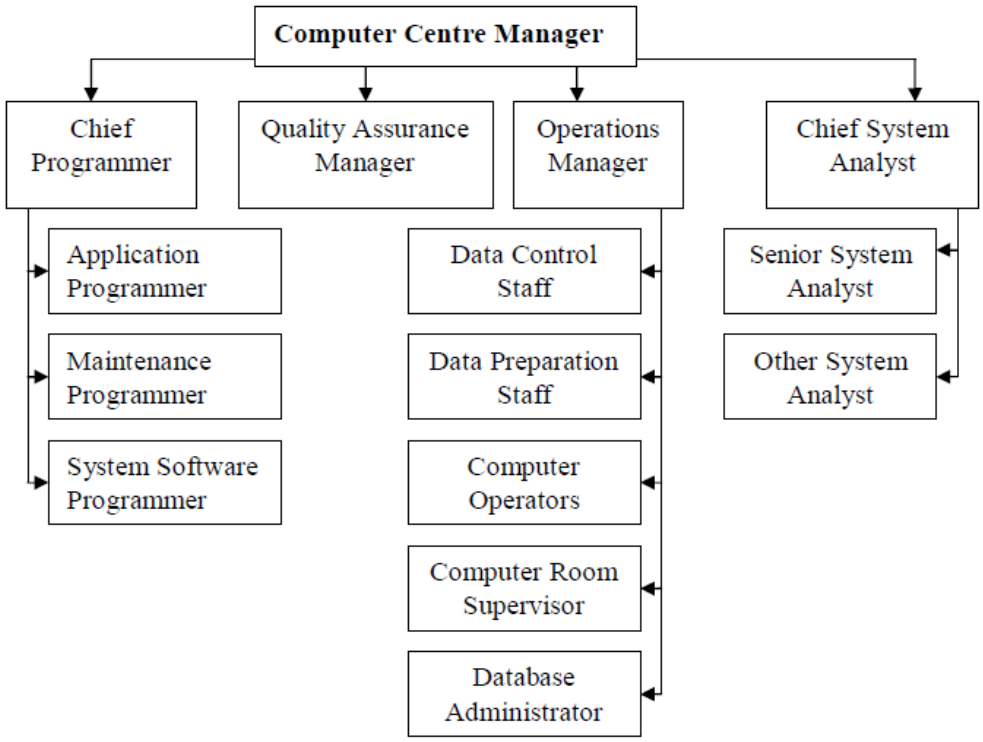

Fig. 2. Data Processing Department Structure II

2.1 PERSONNEL'S FUNCTIONS WITHIN DATA PROCESSING DEPARTMENT

2.1.1 The Data Processing Manager (DPM)

The DPM is responsible for both research and development and for production. He is also in charge of the following responsibilities:

- co-ordination of the developmental objectives.
- responsible for development policy.
- establishment of an effective communications within the department including documentation and other standards
- provision, utilization and control of resources required within the department.
- communicate with the top management on the progress and challenges of the department.

2.1.2 Chief System Analyst

A system analyst carries out feasibilities study on a system. He works with other individuals within the organization to evaluate their information needs, design computer software and hardware to meet those needs and then implement the information system. He defines error messages to be incorporated and checks to be embedded into the system. He functions as project team leader and supervisor to the system analyst. The duties are to:

- Collect, records and analysis details of existing procedure and systems.
- Prepare computer operating instructions.
- Define error messages to be incorporated.
- Estimate runs timing.
- Specified check and control to be embedded in the new system.
- Define actions required to deal with various conditions arising in the system.

2.1.3 Systems Analyst

The systems analyst is the one that defines data processing problems and designs and implements computerized systems. These roles are perform in consonance with the advice from the Chief programmer. A good system analysts must have above average intelligence, numerical ability and verbal ability.

2.1.4 Chief Programmer

Chief Programmers work closely with the system analyst to either create new software or to review existing programs. He supervises application programmers, maintenance programmers and system software programmers. The programmers are in change of programming (applications) and perform the following other functions:

- preparation of program flowcharts and coding.
- program documentation.
- program testing.
- preparation of operating instrument.
- program maintenance and modification.

2.1.5 Programmer

The programmer designs, writes and tests programs. Job titles may be trainee programmer, junior programmer, senior programmer, software programmer, systems programmer. Programmers often become involved in systems analysis and design as members of a systems development team or as advisers on technical subjects to systems analysts. The characteristics of a good programmer are a 'logical' mind, above average intelligence and ability to concentrate on a fine level of detail.

2.1.6 Computer Operations Manager

He is responsible for the day- to –day running of the computer, control and flow of work, data preparation and distribution, and computer operation and also lias with the engineers during maintenance procedure. He is also required to schedule the workload so as to obtain the best use of the resources to ensure that work progress through the department (receipt of data, data preparation, operation, dispatch and control at all stages) and to maintain all the necessary files. The following specialists work with the operation manager: the data control staff, data preparation staff, database administrators, computer room supervisor and computer operators. He will act as liaison between the operations department and the systems programming functions and as new systems are completed, he will absorb them into his programme of work.

2.1.7 Computer Operators

Operators are the professionals that make use of the computers to do their jobs. They make judicious use of both the hardware and the software, which includes the utility programs e.g. file conversion, file copy, file maintenance and reorganization, sorting, back up files, etc. He is in charge of:

- operating equipment in the computer areas,
- cleaning equipment as laid down,
- processing data as required,
- performing program compilation and tests,
- maintenance of log book in respect of machine performance, utilization and failures,
- liaise with engineers during maintenance period

3.0 Summary

In this unit, you have learnt the introductory concept of data processing, administrative structure of a data processing department and the roles of some personnel in this department. You also learnt that the data processing manager is the head of the department under which you have the others like the computer operator, computer analyst, programmer, operation manager, etc.

4.0 Tutor-Marked Assignment

1. Illustrate with a diagram the administrative structure of the school data processing department or data management centre.
2. Write five responsibilities of each of the following personnel's in the school data processing department
   a. Data Processing Manager (DPM)
   b. System Analyst
   c. Programmer
   d. Computer Operator
   e. Clerk

UNIT 2: **COMPUTER OPERATIONS PROCEDURE**

1.0 Introduction

In this unit, you will learn some of the operational principles of the computer system. Some of the issues to be discuss include; principles and procedures of operating the computer system, functions of operating system and storage devices.

2.0 Operating system principles and operation

In previous course like "Introduction to Computer", you will probably have discussed what an operating system is. If not, an operating system is a system software that performs various functions that helps you make good use of your computer system. It allocates resources to your computer hardware and provides the environment to run your applications.

Often as you ON your computer, it's nice to think that you're in control. There's the trusty computer mouse, which you can move anywhere on the screen, summoning up your music library or Internet browser at the slightest whim. Although it's easy to feel like a director in front of your desktop or laptop, there's a lot going on inside, and the real man behind the curtain handling the necessary tasks is the operating system.

Most desktop or laptop PCs come pre-loaded with Microsoft Windows like Window 7 or the latest Window 10 operating system. Macintosh computers come pre-loaded with Mac OS X. Many corporate servers use the Linux or UNIX operating systems. The operating system (OS) is the first thing loaded onto the computer. Without the operating system, a computer is useless.

When a brand new computer comes off the factory assembly line, it can do nothing. The hardware needs software to make it work. Are we talking about applications software such as word processing or spreadsheet software? But an applications software package does not communicate directly with the hardware. As shown in Figure 1, between the applications software and the hardware is a software interface; an *operating system*.

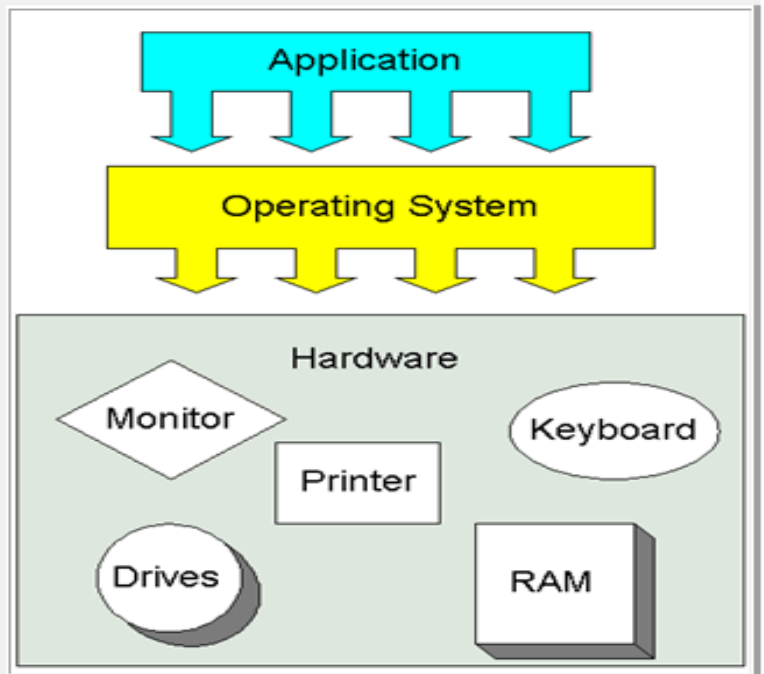

Fig. 1: The Operating System in a Hierarchy

More recently, operating systems have started to pop up in smaller computers as well. If you like to tinker with electronic devices, you're probably pleased that operating systems can now be found on many of the devices we use every day, from cell phones to wireless access points. The computers used in these little devices have gotten so powerful that they can now actually run an operating system and applications. The computer in a typical modern cell phone is now more powerful than a desktop computer from 20 years ago, so this progression makes sense and is a natural development.

2.1 Types of Operating system

Within the broad family of operating systems, there are generally four types, categorized based on the types of computers they control and the sort of applications they support. The categories are:

- **Real-time operating system** (RTOS) - Real-time operating systems are used to control machinery, scientific instruments and industrial systems. An RTOS typically has very little user-interface capability, and no end-user utilities, since the system will be a "sealed box" when delivered for use. A very important part of an RTOS is managing

the resources of the computer so that a particular operation executes in precisely the same amount of time, every time it occurs. In a complex machine, having a part move more quickly just because system resources are available may be just as catastrophic as having it not move at all because the system is busy.

- **Single-user, single task** - As the name implies, this operating system is designed to manage the computer so that one user can effectively do one thing at a time. The Palm OS for Palm handheld computers is a good example of a modern single-user, single-task operating system.
- **Single-user, multi-tasking** - This is the type of operating system most people use on their desktop and laptop computers today. Microsoft's Windows and Apple's MacOS platforms are both examples of operating systems that will let a single user have several programs in operation at the same time. For example, it's entirely possible for a Windows user to be writing a note in a word processor while downloading a file from the Internet while printing the text of an e-mail message.
- **Multi-user** - A multi-user operating system allows many different users to take advantage of the computer's resources simultaneously. The operating system must make sure that the requirements of the various users are balanced, and that each of the programs they are using has sufficient and separate resources so that a problem with one user doesn't affect the entire community of users. Unix, VMS and mainframe operating systems, such as *MVS*, are examples of multi-user operating systems.

2.2 Operating system procedure

When you turn on the power to a computer, the first program that runs is usually a set of instructions kept in the computer's read-only memory (ROM). This code examines the system hardware to make sure everything is functioning properly. This **power-on self test** (POST) checks the CPU, memory, and basic input-output systems (BIOS) for errors and stores the result in a special memory location. Once the POST has successfully completed, the software loaded in ROM (sometimes called the BIOS or **firmware**) will begin to activate the computer's disk drives. In most modern computers, when the computer activates the hard disk drive, it finds the first piece of the operating system: the **bootstrap loader**.

The bootstrap loader is a small program that has a single function: It loads the operating system into memory and allows it to begin operation. In the most basic form, the bootstrap loader sets up the small driver programs that interface with and control the various hardware subsystems of the computer. It sets up the divisions of memory that hold the operating system, user information and applications. It establishes the data structures that will hold the myriad signals, flags and semaphores that are used to communicate within and between the subsystems and applications of the computer. Then it turns control of the computer over to the operating system.

3.0 Computer Storage devices

Memory, which is composed of one or more chips on the motherboard, is a temporary holding place for data and instructions during processing. The contents of **volatile memory**, such as RAM, are lost when the power to the computer is turned off. The contents of **nonvolatile memory**, such as ROM, are not lost when power is removed from the computer.

Computer Storage device holds items such as data, instructions, and information for future use; that is, they holds these items while they are not being processed. It is nonvolatile, which means the items in them retained even when power is removed from the computer. Compared to memory, the **access time** (the time it takes to locate a single item) for them is slow. A **storage medium** (media is the plural) is the physical material on which items are kept. Storage devices can function as sources of input and output. When storage devices transfer items from a storage medium into memory – a process called **reading** – they function as sources of input. When storage devices transfer items from memory to a storage medium – a process called **writing** – they function as sources of output. Types of storage media include floppy disks, hard disks, USB drive, compact discs, tape, PC Cards, microfilm, and microfiche.

3.1 Computer Storage device benefits

The benefits of storage devices can be summarized as follows:

- **Capacity.** Organizations may store the equivalent of a roomful of data on sets of disks that take up less space than a breadbox. A simple diskette for a personal computer

holds the equivalent of 500 printed pages, or one book. An optical disk can hold the equivalent of approximately 400 books.

- **Reliability.** Data in secondary storage is basically safe, since secondary storage is physically reliable. Also, it is more difficult for unscrupulous people to tamper with data on disk than data stored on paper in a file cabinet.
- **Convenience.** With the help of a computer, authorized people can locate and access data quickly.
- **Cost.** Together the three previous benefits indicate significant savings in storage costs. It is less expensive to store data on tape or disk (the principal means of secondary storage) than to buy and house filing cabinets. Data that is reliable and safe is less expensive to maintain than data subject to errors. But the greatest savings can be found in the speed and convenience of filing and retrieving data.

These benefits apply to all the various secondary storage devices but, as you will see, some devices are better than others. Out of all the computer storage devices, Hard disks are the most effective for longer and large storage.

4.0 Summary

In this unit, we have discussed various operations relating to the computer operating system and computer storage devices.

5.0 Tutor-Marked Assignment

1. List four (4) operating systems used in a computer system or mobile device and discuss their mode of operation.
2. Describe how a hard disk organizes data.
3. Differentiate between CD-ROMs, CD-RWs, and DVD-ROMs.
4. Explain how to use PC Cards and other Miniature Storage Media

UNIT 3: **DATA PREPARATION METHODS**

1.0 Introduction

Data Preparation involves checking or logging the data in, checking the data for accuracy, entering the data into the computer, transforming the data and developing and documenting a database structure that integrates the various measures.

2.0 Logging the Data

In any research project, institution that have students, organization that has people there will be data coming from a number of different sources at different times:

- mail surveys returns
- coded interview data
- pretest or posttest data
- observational data
- student exam results
- people's profile
- staff record
- etc

In all these, you need to set up a procedure for logging the information and keeping track of it until you are ready to do a comprehensive data analysis. Different organization differs in how they prefer to keep track of incoming data or record. In most cases, you will want to set up a database that enables you to assess at any time what data is already in and what is still outstanding. You could do this with any standard computerized database program (e.g., Microsoft Access, SQL, Claris Filemaker), although this requires familiarity with such programs or, you can accomplish this using standard statistical programs (e.g., SPSS, SAS, Minitab, Datadesk) and running simple descriptive analyses to get reports on data status. It is also critical that the data analyst retain the original data records for a reasonable period of time. Most professional will retain such records for at least 5-7 years. For important or expensive studies, the original data might be stored in a data archive. The data analyst should always

be able to trace a result from a data analysis back to the original forms on which the data was collected. A database for logging incoming data is a critical component in good research record-keeping.

2.1 Checking the Data for Accuracy

As soon as data is received it should be screen for accuracy. In some circumstances doing this right away will allow you to go back to the sample to clarify any problems or errors. There are several questions that should be asked as part of this initial data screening:

- Are the responses legible/readable?
- Are all important questions answered?
- Are the responses complete?
- Are the records complete?
- Is all relevant contextual information included (e.g., data, time, place, researcher)?

In most social research, quality of measurement is a major issue. Assuring that the data collection process does not contribute inaccuracies will help assure the overall quality of subsequent analyses.

2.2 Developing a Database Structure

The database structure is the manner in which you intend to store the data so that it can be accessed in subsequent data analyses or for viewing. You might use the same structure you used for logging in the data or, in large complex studies or process; you might have one structure for logging data and another for storing it. As mentioned above, there are generally two options for storing data on computer; database programs and statistical programs. Usually database programs are the more complex of the two to learn and operate, but they allow the analyst greater flexibility in manipulating the data.

In every research project, you should generate a printed **codebook** that describes the data and indicates where and how it can be accessed. Minimally the codebook should include the following items for each variable:

- variable name

- variable description
- variable format (number, data, text)
- instrument/method of collection
- date collected
- respondent or group
- variable location (in database)
- notes

The codebook is an indispensable tool for the analysis team. Together with the database, it should provide comprehensive documentation that enables other researchers who might subsequently want to analyze the data to do so without any additional information.

2.3 Entering the Data into the Computer

There are a wide variety of ways to enter the data into the computer for analysis or for record storage. Probably the easiest is to just type the data in directly. In order to assure a high level of data accuracy, the computer analyst should use a procedure called **double entry**. In this procedure, you enter the data once. Then, you use a special program that allows you to enter the data a second time and checks each second entry against the first. If there is a discrepancy, the program notifies the user and allows the user to determine the correct entry. This double entry procedure significantly reduces entry errors. However, these double entry programs are not widely available and require some training. An alternative is to enter the data once and set up a procedure for checking the data for accuracy. For instance, you might spot check records on a random basis.

Once the data have been entered, you will use various programs to summarize the data that allow you to check that all the data are within acceptable limits and boundaries. For instance, such summaries will enable you to easily spot whether there are persons whose age is 601 or who have a 7 entered where you expect a 1-to-5 response.

2.4 Data Transformations

Once the data have been entered it is almost always necessary to transform the raw data into variables that are usable in the analyses. There are a wide variety of transformations that you might perform. Some of the more common are:

- missing values

  Many analysis programs automatically treat blank values as missing. In others, you need to designate specific values to represent missing values. For instance, you might use a value of -99 to indicate that the item is missing. You need to check the specific program you are using to determine how to handle missing values.

- item reversals

  On scales and surveys, we sometimes use **reversal items** to help reduce the possibility of a response set. When you analyze the data, you want all scores for scale items to be in the same direction where high scores mean the same thing and low scores mean the same thing. In these cases, you have to reverse the ratings for some of the scale items.

- scale totals

  Once you've transformed any individual scale items you will often want to add or average across individual items to get a total score for the scale.

- categories

  For many variables you will want to collapse them into categories. For instance, you may want to collapse income estimates (in naira amounts) into income ranges.

3.0 SUMMARY

In this unit, we have discussed most of the necessary techniques required for data preparation and data analysis. You should understand that the main reason for gathering data is to process them into useful information. So, adequate effort must be put in place to ensure the data is accurate, complete and well organized.

4.0 Tutor-Marked Assignment

1. Write a comprehensive note on any two database program and data analysis program.

UNIT 4: **COMPUTER SECURITY**

1.0 Introduction

The meaning of the term *computer security* has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons:

- To prevent theft or damage to the hardware
- To prevent theft or damage to the information
- To prevent disruption of service

Strict procedures for access to the computer room are used by most organizations, and these procedures are often an organization's only obvious computer security measures. Today, however, with pervasive remote terminal access, communications, and networking, physical measures rarely provide meaningful protection for either the information or the service; only the hardware is secure. Nonetheless, most computer facilities continue to protect their physical machine far better than they do their data, even when the value of the data is several times greater than the value of the hardware.

Computer security, also known as **cybersecurity** or **IT security**, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

The field is of growing importance due to the increasing reliance on computer systems in most societies and the growth of "smart" devices, including smartphones, televisions and tiny

devices as part of the Internet of Things – and of the Internet and wireless network such as Bluetooth and Wi-Fi.

2.0 Computer Vulnerabilities and attacks

Computer vulnerability is a system susceptibility or flaw. To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the following categories:

I. Backdoors

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may also have been added later by an authorized party to allow some legitimate access or by an attacker for malicious reasons; but regardless of the motives for their existence, they create vulnerability.

II. Denial-of-service attack (DoS)

Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

III. Direct-access attacks

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making operating

system modifications, installing software worms, keyloggers, covert listening devices or using wireless mice. Even when the system is protected by standard security measures, these may be able to be by passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

IV. Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and Narus Insight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

V. Spoofing

Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a high level of security.

VI. Tampering

Tampering describes a malicious modification of products. So-called "Evil Maid" attacks and security services planting of surveillance capability into routers are examples.

VII. Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. So for example a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.

VIII. Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or

instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Preying on a victim's trusting, phishing can be classified as a form of social engineering.

IX. Clickjacking

Clickjacking, also known as "UI redress attack or User Interface redress attack", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "hijacking" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

X. Social engineering

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer. A popular and profitable cyber scam involves fake CEO emails sent to accounting and finance departments. In early 2016, the FBI reported that the scam has cost US businesses more than $2bn in about two years. In May 2016, the Milwaukee Bucks NBA team was the victim of this type of cyber scam with a perpetrator impersonating the team's president Peter Feigin, resulting in the handover of all the team's employees' 2015 W-2 tax forms.

2.1 Computer Security risk targets

Computer security is critical in almost any industry which uses computers. Currently, most electronic devices such as computer, laptops and cellphones come with built in firewall security software, but despite this, computers are not 100 percent accurate and dependable to protect our data. There are many different ways of hacking into computer, it can be done through network system, clicking into unknown links, connecting unfamiliar Wi-Fi, download software and files from unsafe sites, power consumption, electromagnetic radiation waves

and many more. However, computer can be protected through well build software and hardware. Such as having strong internal interactions of properties of the software complexity can prevent software crash and security failure. Some of the well-known security targets are discussed below:

I. Financial systems

Web sites and apps that accept or store credit card numbers, brokerage accounts, and bank account information are prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the black market. In-store payment systems and ATMs have also been tampered with in order to gather customer account data and PINs.

II. Utilities and industrial equipment

Computers control functions at many utilities, including coordination of telecommunications, the power grid, nuclear power plants, and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the Stuxnet worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable to physical damage caused by malicious commands sent to industrial equipment which are infected via removable media.

III. Aviation

The aviation industry is very reliant on a series of complex system which could be attacked. A simple power outage at one airport can cause repercussions worldwide, much of the system relies on radio transmissions which could be disrupted, and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore. There is also potential for attack from within an aircraft. The consequences of a successful attack range from loss of confidentiality to loss of system integrity, which may lead to more serious concerns such as exfiltration of data, network and air traffic control outages, which in turn can lead to airport closures, loss of aircraft, loss of passenger life, damages on the ground and to transportation infrastructure. A successful attack on a military aviation system that controls munitions could have even more serious consequences.

IV. Consumer devices

Desktop computers and laptops are commonly infected with malware either to gather passwords or financial account information, or to construct a botnet to attack another target. Smart phones, tablet computers, smart watches, and other mobile devices such as Quantified Self devices like activity trackers have also become targets and many of these have sensors such as cameras, microphones, GPS receivers, compasses, and accelerometers which could be exploited, and may collect personal information, including sensitive health information. Wifi, Bluetooth, and cell phone network on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach. Home automation devices such as the Nest thermostat are also potential targets.

V. Large corporations

Large corporations are common targets. In many cases this is aimed at financial gain through identity theft and involves data breaches such as the loss of millions of clients' credit card details by Home Depot, Staples and Target Corporation. Medical records have been targeted for use in general identifies theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale.

VI. Automobiles

If access is gained to a car's internal controller area network, it is possible to disable the brakes and turn the steering wheel. Computerized engine timing, cruise control, anti-lock brakes, seat belt tensioners, door locks, airbags and advanced driver assistance systems make these disruptions possible, and self-driving cars go even further. Connected cars may use wifi and bluetooth to communicate with onboard consumer devices, and the cell phone network to contact concierge and emergency assistance services or get navigational or entertainment information; each of these networks is a potential entry point for malware or an attacker. Researchers in 2011 were even able to use a malicious compact disc in a car's stereo system as a successful attack vector and cars with built-in voice recognition or remote assistance features have onboard microphones which could be used for eavesdropping.

VII. Government

Government and military computer systems are commonly attacked by activists and foreign powers. Local and regional government infrastructure such as traffic light controls, police and intelligence agency communications, personnel records, student records and financial systems are also potential targets as they are now all largely computerized. Passports and government ID cards that control access to facilities which use RFID can be vulnerable to cloning.

3.0 Computer Security attack protection (countermeasure)

In computer security a countermeasure is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. Some common countermeasures are listed in the following below:

3.1 Security measures

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- 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. Firewalls can be both hardware- or software-based.
- Intrusion Detection System (IDS) products 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, as it may happen that not all the compromised resources are detected.

3.2 Reducing vulnerability

While formal verification of the correctness of computer systems is possible, it is not yet common. Operating systems formally verified include seL4, and SYSGO's PikeOS – but these make up a very small percentage of the market. Computer security vulnerability can be minimized or reduced using some of this approach:

- Cryptography properly implemented is now virtually impossible to directly break. 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.
- Two factor authentication is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or other piece of hardware. This increases security as an unauthorized person needs both of these to gain access.
- 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. Training is often involved to help mitigate this risk, but even in a highly disciplined environments (e.g. military organizations), social engineering attacks can still be difficult to foresee and prevent.
- It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, 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.

3.3 **Computer Hardware protection mechanisms**

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process, hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as dongles, trusted platform modules, intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated backdoor access) required in order to be compromised. Each of these is covered in more detail below.

- USB dongles are typically used in software licensing schemes to unlock software capabilities, but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as Advanced Encryption Standard (AES) provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or Virtual Private Networks (VPNs). In addition, a USB dongle can be configured to lock or unlock a computer.
- Trusted platform modules (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.
- Computer case intrusion detection refers to a push-button switch which is triggered when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.
- Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves. Tools exist specifically for encrypting external drives as well.

- Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.
- Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as Bluetooth, the newer Bluetooth low energy (LE), Near field communication (NFC) on non-iOS devices and biometric validation such as thumb print readers, as well as QR code reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.

4.0 SUMMARY

So much has been learnt in this unit about computer security breaches and prevention, it is pertinent to note that security assurance is of utmost important in this era of anonymous security breach.

5.0 Tutor-Marked Assignment

1. Discuss any available hardware and software means of protecting computer against unauthorized attack.
2. Discuss what you understand by a cyber-attack.
3. Why is computer security so important?

UNIT 5: **COMPUTER FILE STRUCTURE**

1.0 Introduction

A **computer file** is a resource for storing information, which is available to a computer program and is usually based on some kind of durable storage. A file is "durable" in the sense that it remains available for other programs to use after the program that created it has finished executing. Computer files can be considered as the information technology counterpart of paper documents which traditionally are kept in office and library files.

A file is also a collection of data stored on mass storage (e.g., disk or tape). Why on mass storage? It will be too big to fit in main memory and the possibility to share the data between programs backup. The data is in a file can be subdivided into records (e.g., student information). Each record contains a number of fields (e.g., name, GPA). One (or more) field is the key field (e.g., name). File is of various forms; sequential files, indexed files, and hashed files.

i. Sequential files

Sequential Files Records are conceptually organized in a sequential list and can only be accessed sequentially. The actual storage might or might not be sequential: On a tape, it usually is. On a disk, it might be distributed across sectors and the operating system would use a linked list of sectors to provide the illusion of sequentiality. Convenient way to batch (group together) a number of updates are to:

- Store the file in sorted order of key field.
- Sort the updates in increasing order of key field.
- Scan through the file once, doing each update in order as the matching record is reached.

ii. Indexed Files

Sequential search is slower on disk/tape than in main memory. Improving the performance is mostly through more sophisticated data structures. An index for a file is a list of key field

values occurring in the file along with the address of the corresponding record in the mass storage. Typically the key field is much smaller than the entire record, so the index will fit in main memory. The index can be organized as a list, a search tree, a hash table, etc. To find a particular record:

- the index is search for the desired key.
- When the search returns the index entry, the record's is extracted from its address on mass storage.
- The mass storage can be access at the given address to get the desired record.

Multiple indexes, one per key field, allow searches based on different fields.

iii. Hashed Files

An alternative to storing the index as a hash table is to not have an index at all. Instead, hash on the key to find the address of the desired record and use open addressing to resolve collisions.

2.0 File contents

On most modern operating systems, files are organized into one-dimensional arrays of bytes. The format of a file is defined by its content since a file is solely a container for data, although, on some platforms the format is usually indicated by its filename extension, specifying the rules for how the bytes must be organized and interpreted meaningfully. For example, the bytes of a plain text file (.txt in Windows) are associated with either ASCII or UTF-8 characters, while the bytes of image, video, and audio files are interpreted otherwise. Most file types also allocate a few bytes for metadata, which allows a file to carry some basic information about itself. Some file systems can store arbitrary (not interpreted by the file system) file-specific data outside of the file format, but linked to the file, for example extended attributes or forks.

2.1 Organization of data in a file

Information in a computer file can consist of smaller packets of information (often called "records" or "lines") that are individually different but share some common traits. For example, a payroll file might contain information concerning all the employees in a company and their payroll details; each record in the payroll file concerns just one employee, and all the records have the common trait of being related to payroll—this is very similar to placing all payroll information into a specific filing cabinet in an office that does not have a computer. A text file may contain lines of text, corresponding to printed lines on a piece of paper. Alternatively, a file may contain an arbitrary binary image (a BLOB) or it may contain an executable. The way information is grouped into a file is entirely up to how it is designed. This has led to a plethora of more or less standardized file structures for all imaginable purposes, from the simplest to the most complex. Most computer files are used by computer programs which create, modify or delete the files for their own use on an as-needed basis. The programmers who create the programs decide what files are needed, how they are to be used and (often) their names.

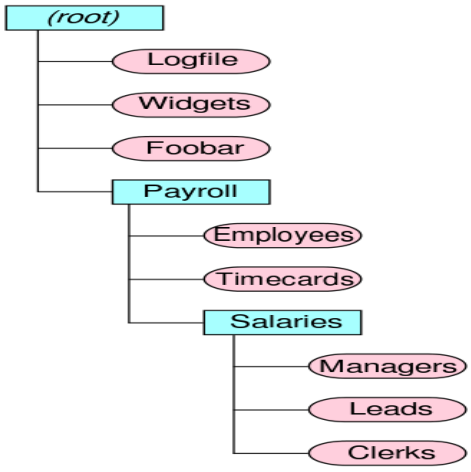

Fig. 1. Files and folders arranged in a hierarchy

2.2 File Operations

The most basic operations that programs can perform on a file are:

- Create a new file
- Change the access permissions and attributes of a file

- Open a file, which makes the file contents available to the program
- Read data from a file
- Write data to a file
- Close a file, terminating the association between it and the program

Files on a computer can be created, moved, modified, grown, shrunk, and deleted. In most cases, computer programs that are executed on the computer handle these operations, but the user of a computer can also manipulate files if necessary. For instance, Microsoft Word files are normally created and modified by the Microsoft Word program in response to user commands, but the user can also move, rename, or delete these files directly by using a file manager program such as Windows Explorer (on Windows computers) or by command lines (CLI).

2.3 File Protection

Many modern computer systems provide methods for protecting files against accidental and deliberate damage. Computers that allow for multiple users implement file permissions to control who may or may not modify, delete, or create files and folders. For example, a given user may be granted only permission to read a file or folder, but not to modify or delete it; or a user may be given permission to read and modify files or folders, but not to execute them. Permissions may also be used to allow only certain users to see the contents of a file or folder. Permissions protect against unauthorized tampering or destruction of information in files, and keep private information confidential from unauthorized users.

Another protection mechanism implemented in many computers is a *read-only flag.* When this flag is turned on for a file (which can be accomplished by a computer program or by a human user) the file can be examined, but it cannot be modified. This flag is useful for critical information that must not be modified or erased, such as special files that are used only by internal parts of the computer system. Some systems also include a *hidden flag* to make certain files invisible; this flag is used by the computer system to hide essential system files that users should not alter.

2.4 File Storage

Any file that has any useful purpose must have some physical manifestation. That is, a file (an abstract concept) in a real computer system must have a real physical analogue if it is to exist at all. In physical terms, most computer files are stored on some type of data storage device. For example, most operating systems store files on a hard disk. Computer files can be also stored on other media in some cases, such as magnetic tapes, compact discs, Digital Versatile Discs, Zip drives, USB flash drives, etc. The use of solid state drives is also beginning to rival the hard disk drive.

Bibliography

1. Wooldridge, S. (2013). *Data Processing: Made Simple*. Elsevier.
2. http://computer.howstuffworks.com/
3. http://www.socialresearchmethods.net/kb/statprep.php