ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-021
INTRODUCTION TO INFORMATION SECURITY

Business Needs & Security Awareness

1

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्र की भावनौ का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।"

— इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barries of caste and class, smoothing out inequalities imposed by birth and other circumstances."

— Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSEI-021
Introduction to Information Security

Block

1

BUSINESS NEEDS AND SECURITY AWARENESS

Programme Expert/Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Block Preparation

Unit Writers

Mr. Kaushal Mehta, Assistant Professor
Bhai Parmanand of Business Studies
Shakarpur, Delhi (Unit 1)

Mr. Rajiv Ranjan Singh, Assistant Professor
Department of Computer Science
Shyamlal College (Eve) (DU) (Unit 2)

Mr. Arun Bakshi
Sr. Assistant Professor (IT)
Gitaratan International Business School
Madhuban Chowk, Delhi (Unit 3 & 4)

Block Editor

Prof. K.R. Srivathsan
Pro Vice-Chancellor
IGNOU

Ms. Urshla Kant
Assistant Professor
School of Vocational
Education & Training
IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor
School of Vocational
Education & Training
IGNOU

Production

Mr. B. Natrajan
Dy. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Jitender Sethi
Asstt. Registrar (Pub.)
MPDD, IGNOU, New Delhi

Mr. Hemant Parida
Proof Reader
MPDD, IGNOU, New Delhi

August, 2011

ISBN : 978-81-266-5565-6

Further information about the School of Vocational Education and Training and the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110068. or the website of IGNOU www.ignou.ac.in

Printed and published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD

Laser typeset by Mctronics Printographics, 27/3 Ward No. 1, Opp. Mother Dairy, Mehrauli, New Delhi-30

Printed by : Hi-Tech Graphics, S-39, Okhla Industrial Area, Phase-II, New Delhi-110020

COURSE INTRODUCTION

This course introduces many of the concepts and terms which are most important in gaining an understanding of Information Security. It focuses on techniques for achieving access control within computer systems and networks. The course begins by focusing on business needs and security awareness. It is the fundamental need to spread the word of information security among the netizens for raising the degree of protection. This course emphasize on the importance of information security in order to ensure that only specific authorized users are allowed to access control over information on a computer.

This course has given much emphasize on the basic security threats which affect computer at a rapid rate such as viruses, worms, Trojan horses, hacking etc. The knowledge as to the security threats clears the vulnerabilities as such which may affect network management. This course further elaborates over the networking concepts and protocol for the proper understanding of means for transmitting of a security threats. This course focuses on the concepts and terms related to the security of operation system. It covers the topic related to authentication, access controls, security models, integrity checks or antivirus software.

How the security is compromised and what are the loopholes available in our Operating System, will be discussed in detail. Feasible improvements to the security of an existing operating system, as well as fundamental limitations on those improvements, are also well described.

This course certainly defines all Concepts and Terminology for Information Security; also it addresses concepts and terminology for network and operation system security. It address concepts and terms that we consider to be the most critical to gain a fundamental understanding of Information security technology that is, the theory of this technology and something of its implementation. Our approach in this course is to focus primarily on explaining concepts critical to understanding Computer and Information Security.

The terminologies explained in this course will also provide an insight about the best possible ways to secure our infrastructure, software, Information, Operating system, Emails, Data, Servers, Browsers etc. from the professional crackers who always try to misuse such things for committing Cyber-Crimes. It will also explain the "Information Technology Act" in detail where all the Cyber-Crimes are mentioned along with their penalty and punishment as well. The entire course has been divided into various Blocks/ Sections which focus on identifying the domain of this course for the concepts and terminology discussed. They clarify what we mean by just one term – Information Security.

This course includes the following blocks:

Block 1 - Business Needs and Security Awareness

Block 2 - Security Threat and Vulnerability

Block 3 - Networking Concepts and Attacks

Block 4 - Operating System Concepts

BLOCK INTRODUCTION

We use computers practically for most of our jobs lives these days and hence are too much dependent on them. We use them as tools for work, data storage, schoolwork, shopping, and entertainment. As a lot of important information is always stored on our computers we have to make sure they are protected from any kind of loss of information. Businesses also have to secure information on their computers to protect it from various forms of attacks day and night. The PC of an individual user is also not safe anymore as most of the PCs are part of a big network i.e. Internet and hence open to all kind of attacks from various sources. Although we can't expect all computer users to be technically sound to handle all the security related issues themselves, we can at least make them aware about the security issues and other impact factors that may be critical to the mission of an organisation. The "Security Awareness" or "Information security Awareness" is an activity simply to focus attention on security. Awareness programs are intended to allow individuals to recognise IT security concerns and respond accordingly. This block comprises of four units and is designed in the following way;

The **Unit one** covers the detailed descriptions of all the necessary features of Information technology. Information technology, usually abbreviated as IT, is defined as the umbrella covering all activities associated with computer based information systems. It is defined as the study, design, development, implementation, support or management of computer based information systems. This unit actually deals with how to use computer software and hardware and computer networks to produce, store, protect, process, transmit, and retrieve securely and efficiently the information.

The **Unit two** presents the need of Security Awareness from a point of view of both the end user as well as the organisation, be it the government or an enterprise. It outlines the fundamentals of Security Awareness where the need and justification of having an awareness programme is presented. It also covers the security awareness program life cycle that includes awareness program design, materials development, program implementation and post implementation activities.

The **Unit three** explains that Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review. This makes information security an indispensable part of all the business operations across different domains.

Unit four is an effort towards covering some of the important topics related to legal and ethical issues of business, especially with respect to online business. The learner will be able to learn about security disciplines to safeguard sensitive, legal, ethical and regulatory issues. Learner will also know about the ethical issues with respect to employer and employees perspective. Issues related with advertisement and topics like gender discrimination in the workplace are also covered. Finally the topics like business security policies & procedures, ethical and legal issues of e-commerce are also discussed.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 INFORMATION TECHNOLOGY CONCEPT AND APPLICATION

Structure

1.0 INTRODUCTION

Information technology (IT) is the acquisition, processing, storage and dissemination of vocal, pictorial, textual and numerical information by a microelectronics-based combination of computing and telecommunications. It is the area of managing technology and spans wide variety of areas that include but are not limited to things such as processes, computer software, information systems, computer hardware, programming languages and data constructs. In short, anything that renders data, information or perceived knowledge in any visual format whatsoever, via any multimedia distribution mechanism, is considered part of the IT domain. IT provides businesses with four sets of core services to help execute the business strategy: business process automation, providing information, connecting with customers and productivity tools.

1.1 OBJECTIVES

After going through this unit, you should be able to:

- describe information technology;
- understand computers and its classification;

- know computer software and computer security; and
- explain virus and its types.

1.2 INFORMATION TECHNOLOGY

UNESCO defines Information Technology (IT) as "scientific technological engineering disciplines and the management techniques used in information handling and processing, their application, computers and their interaction with men and machines and associated social, economical and cultural matters."

OECD (1987) treats Information Technology as "a term covering technologies used in the collection, processing and transmission of information. It includes micro-electronic and info-electronic-based technologies incorporated in many products and production processes and increasingly affecting the service sector. It covers inter-alia computers, electronic office equipment, telecommunication, industrial robots and computer controlled machines, electronic components and software products."

1.3 COMPUTER

A computer is a high speed, general purpose, digital electronic, stored program data processor, i.e. Computer is an electronic machine that performs a specified sequence of operations as per the set of instructions (programmes) given a set of data (input) to generate desired information (output).

Donald H. Sander defines computer as a fast and accurate, electronic data manipulating system that is designed and organized to automatically accept and store input data, process them and produce output results under the direction of a detailed step-by-step set of instructions (called as program) that is stored internally.

Characteristics of computers

1) Speed
2) Accuracy
3) Storage and Retrieval
4) Repeated Processing Capabilities
5) Reliability
6) Flexibility
7) Diligence

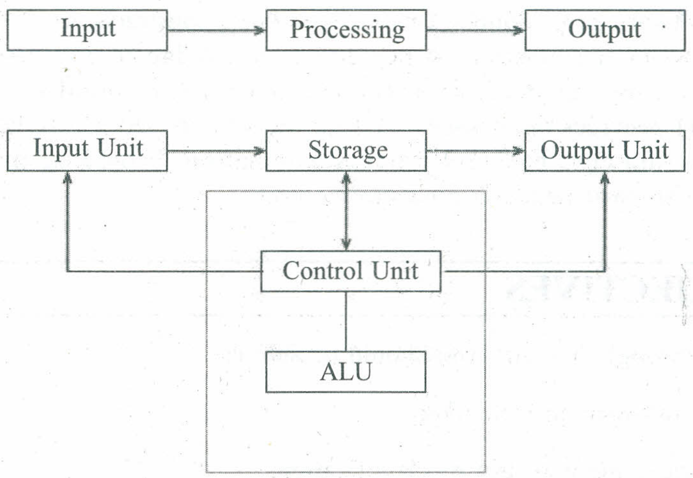


Fig. 1: Diagram of working organization of a computer

Computer operations

A computer's operations are the following:

Input: Data and programmed instructions are input to the computer using appropriate methods.

Storage: Data and instructions are held in computer storage (either in the central processing unit or on back-up storage) until required for processing.

Processing: The necessary arithmetical and logical operations are carried out within the central processing unit (CPU)

Output: The results of processing is output on the required medium/device

Control: The processing steps are controlled by the stored program working in conjuction with the CPU's control unit and the operating systems' programmes. The use of the input and output devices is similarly controlled, while all operations are monitored by the computer operator.

Components of computer

Computer systems are composed of five basic components:

1) Hardware
2) Software
3) User programmes
4) Procedures
5) Data processing personnel

Hardware is the machines used by a data processing department, including data-preparation devices, input and output devices.

Software consists of the collection of programmes and operating aids associated with a computer that facilitate its operation and programming.

User programmes are programmes written by the users of the computers systems.

Procedures are the rules, policies and guidelines governing the operation of the computer centre.

Data processing personnel are the people responsible for keeping the data processing department functioning in an effective and efficient manner.

Classification of computers

The classification of computers is based on the following three criteria:

a) According to purpose
b) According to technology used
c) According to size and capacity

a) According to purpose

1) **General purpose computers:** Computers that follow instructions for general requirements such as sales analysis, financial accounting, invoicing, inventory, management information, etc. are called General Purpose Computers.

2) **Special Purpose Computers:** Computer designed to perform special tasks like scientific applications and research, space applications weather forecasting, medical diagnostics etc. are called Special Purpose Computers.

b) **According to Technology used**

1) **Analog Computers:** Analog computers are computers that measures physical quantities like pressure, temperature, length etc. and convert them to numerical value. They are used for scientific and engineering purpose and they give only approximate results.

2) **Digital Computers:** Most computers are digital devices, i.e. they count the numbers (or digits) that represent numerical or other special symbols.

3) **Hybrid Computers:** Hybrid computers incorporate the technology of both analog and digital computers. These computers store and process analog signals which have been converted into discrete numbers using analog-to-digital converters.

c) **According to Size and Capacity**

1) **Super Computers:** Super computers are huge general purpose computers having a processing capacity of 10,000 mips (millions instruction/sec.), have a storage capacity of millions of bytes. The high speed in these computers is due to use of a number of microprocessors working in parallel and high storage densities are obtained by using magnetic bubble memories and CCDs (Charge Coupled Devices), thus reducing the cost of storage.

2) **Mainframe Computers:** A Mainframe computer is generally a large fast computer system designed for the processing of huge amounts of data.

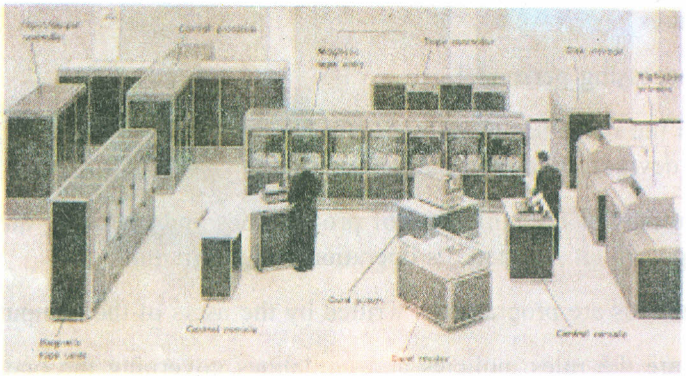


Fig. 2

3) **Minicomputers:** Minicomputers are small versions of the mainframe computers. Like mainframes they have many terminals which are connected with one CPU and can support many users. The capacity of the central processing unit and peripheral devices is comparatively less than those of the mainframe computers.

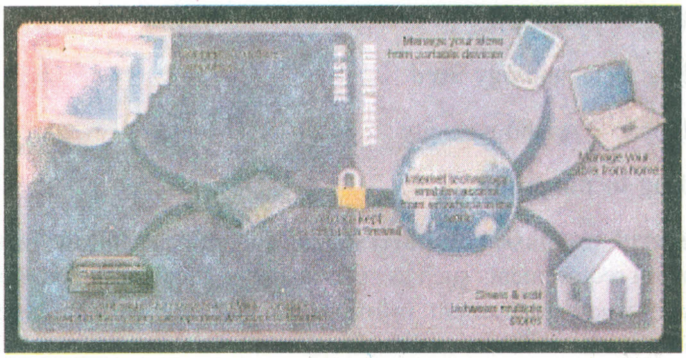


Fig. 3

4) **Microcomputers:** Microcomputers appeared due to technological advances in fabricating highly miniaturized silicon chips. These computers use microprocessor that is why they are called microcomputers.

1.4 APPLICATION AREAS OF COMPUTERS

Computers are used in the following areas: Science and Technology, Business, Industry, Manufacturing, Transport and Communication, Telecommunication, Medicine and health care, Education, banking, Law and order, Publishing Industry, Engineering Technologies.

Data representation

The computers handle the data by electrical components like translators, semiconductors, integrated circuits or wires which exist in two states. A transistor may be conducting or non-conducting, magnetic material like ferrite cores may be magnetized in one direction or the other and a wire may or may not be carrying a current. Thus a computer can understand only one language consisting of two symbols. The binary language, known as the machine language, is best suited for this purpose as it consists of only two symbols 0 and 1. Unfortunately, the most common way to represent the data is the use of numerals 0 to 9 and the alphabets A to Z along with some special symbols like +, -, × and /, etc. the computer is unable to understand and supplied data represented by these symbols. The limitation of a computer to understand the human language necessitated the changing of data to binary form, known as coding of data. This enables the communication between a computer and a human being.

Why the binary system?

Electronic components by their vary nature, operate in binary mode. A switch is either on (1) or off (0) or again, a transistor is either conducting (1) or non-conducting (0). This is generally denoted by Bit, which has been extracted from the two words Binary digit.

Memory and data storage

There are two types of memory in the computer system viz. Primary and Secondary

Primary Storage: Primary storage also known as main memory or core memory, provides capability to store input data, statements from currently undergoing processing, data resulting from processing and data in preparation for output. For example RAM, ROM, PROM, EPROM, EEPROM.

- **RAM (Random Access Memory):** It is a temporary memory and it is used when the program and application is in execution process. RAM is volatile.
- **ROM (Read Only Memory):** It is a permanent memory and can only be read; data cannot be written into it. ROM is permanent and non-volatile.

Secondary Storage: Besides primary storage, where information and programmes are stored for immediate processing, modern computer systems used additional types of storage known as secondary storage, backup storage or auxiliary storage to accomplish their tasks. For example Floppy disk, Hard disk, Pen drives etc.

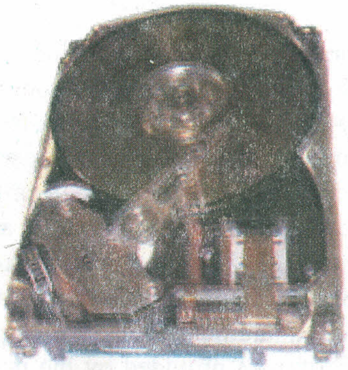


Fig. 4: Hard Disk (Secondary Storage)

Fig. 5: Various storage devices viz. Floppy Drives, Tape, Hard drives, CDs, DVDs, ZIP disks, Memory Keys

Difference between Primary and Secondary storage

Characteristics	Primary Storage	Secondary Storage
1) Location w.r. to CPU	Within CPU	Outside but connected to CPU
2) Cost	Most expensive	Less expensive than primary storage
3) Capacity	Up to several million bits	Billions of bits
4) Access time	In billionths of a second	In millionths of a second
5) Data can be processed directly from storage	Yes	No, must first be routed through primary storage
6) Means of storing information	Semi Conductor	Magnetic tape, magnetic disk, optical disk etc.

Virtual Storage: Virtual storage is a useful processing technique that has emerged in conjunction with systems operating on more than one program at a time. When large programmes are being executed, it is quite possible for insufficient storage to be available to meet the program requirements, particularly when a limited partition or section of memory is available of each program to use. Under this technique, the program is segmented into pages, which are fixed size storage area that contain a number of instructions. Most pages are kept on secondary storage devices and only those actually needed at a particular instant are in primary storage. This means, pages are moved in and out of memory, as program require them, by specially developed control software provided by the manufacturers.

Cache Memory: Cache memory that is both faster and more expensive per character stored than primary storage. This high-speed circuitry is used as "scratch pad" to temporarily store data and instructions that are likely to be retrieved many times during processing.

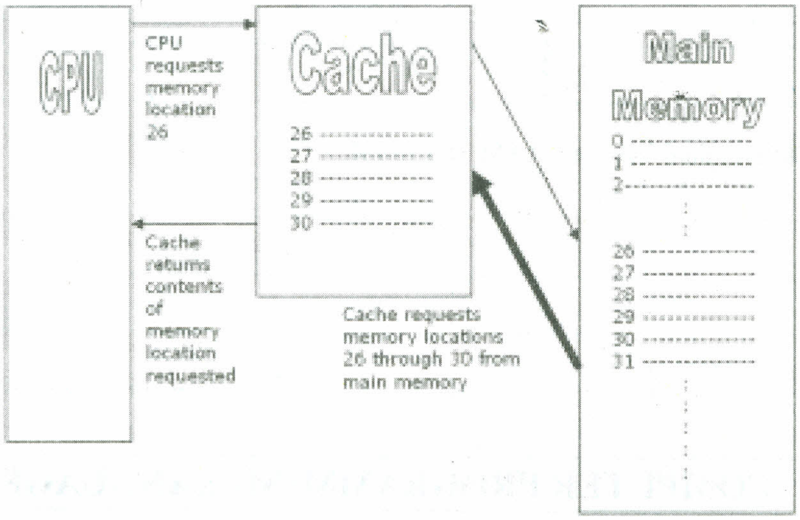


Fig. 6

1.5 COMPUTER SOFTWARE

Definition: Computer software is a sequence of instructions written in a language understood by the computer is called a computer program. A program or a set of programmes is called software.

The computer program that causes general purpose computing equipment to solve specific problems and perform basic functions is known as software.

Classification of Software

There are three types of Software's:

1) **System software:** System software refers to all the programmes that make the computer work. System software manages the resources of the computer such as the Central Processor, Communication links and Input/output devices. For example, assemblers, compilers, interpreters, editors etc.

2) **Application Software:** A program or software develops to solve a problem on a computer is called application software. It refers to software which processes data to structure or automate specific business processes or it consists of programmes which direct computers to perform specific information activities for end users.

3) **Utility Software:** Utility software's are considered as generalized application or system software which is used quiet often in the development of a program or sometimes required to transfer data from tape to tape. Other utility programmes like sort, merge, programmes are used to sort records into a particular sequence to facilitate updating of files. These sorted files can be merged into a single updated file using merge utility program. These utility programmes are flexible to handle user needs.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is computer? Explain its classification.

....

....

....

....

2) Differentiate between RAM and ROM.

....

....

....

....

1.6 COMPUTER PROGRAMMING LANGUAGES

Programming Languages: Programming is the creation of a list of stored instructions that tell a computer what to do and programming language is an artificial language composed of a fixed vocabulary and a set of rules used to create instructions for the computer to follow.

1) **Machine Language:** The computer understands nothing but 0s and 1s and these 0s and 1s makes the machine level language. It is also called low level language. These machine level instructions are divided into two parts:

   Operation (code) and Operand (address)

2) **Assembly Language:** The language which substitutes letters and symbols for the numbers in the machine language program is called an Assembly Language. For example, Add, subtract etc.

3) **High level Languages:** To overcome the low level language difficulty of machine dependency, high level languages were developed. Such programming languages with an extensive vocabulary of words and symbols are used to instruct a computer to carry out the necessary procedures are called High Level Languages, e.g. C, C++.

4) **Fourth Generation Languages:** Fourth generation languages are directly used by the end users and it requires less skilled programmers to develop computer applications. Fourth generation languages tend to be non-procedural or less-procedural. Procedural languages require specification of sequence of steps and non-procedural languages need only to specify what has to be done rather than to provide details about how to carry out the task. Thus a non-procedural language can do the same task with less steps and lines of program code than a procedural language.

5) **Fifth Generation Languages:** These languages represent the next natural language programming. Natural language eliminates the need for the user or programmer to learn a specific vocabulary, grammar or syntax of a language. The statements of a natural language are similar to human speech.

Characteristics of a good programming languag

1) A good programming language should be easy to understand.

2) The structu re of the language should be very simple and it should have a very simple syntax.

3) It should have availability of appropriate data structure so that solving a given problem may be quiet easy.

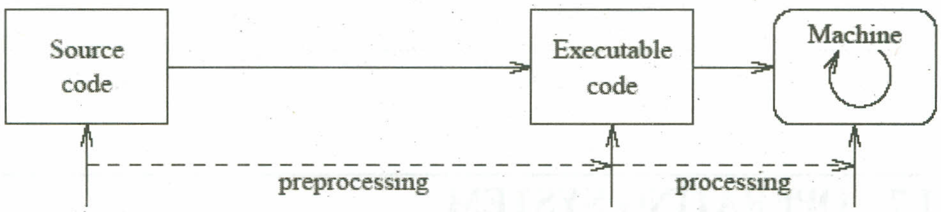
4) It should have presence of appropriate support environment and functions such as editors and extra library functions.

5) It should be easy to verify and modify thus reducing the program development time and increase the efficiency of the resultant software.

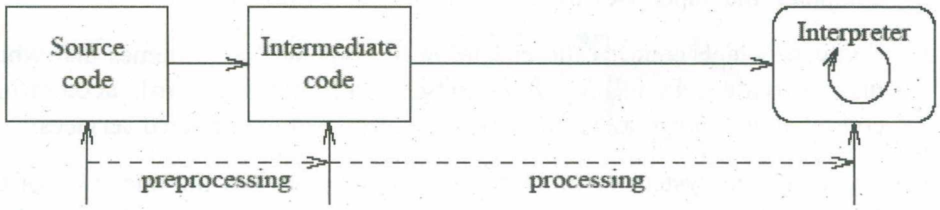
Language translators programmes

Compiler: A computer program that produces a machine language program from source program. It converts whole program together into machine level language. For example, compiler of C.

Interpreter: A computer program that translates each source language statement into a sequence of machine instructions line by line. For example, Basic.



Compilation



Interpretation

Fig. 7

Difference between interpreter and compiler

Interpreter	**Compiler**
1) Translates the program line by line	1) Translates the entire program
2) Requires less main memory	2) Requires more main memory
3) Each time the program is executed every line is checked for syntax and then converted into equivalent machine code	3) Converts the entire program to machine code when all the syntax errors are removed and executes the object code directly
4) Source program and the interpreter requires for execution	4) Neither source nor the compiler are required for execution
5) Good for fast debugging and at testing stage	5) Slow for debugging and testing
6) Execution time is more	6) Execution time is less
7) No security of source code	7) Security of source code

Debugging: The process of eliminating all errors and suitable modifying instructions to help the process is called debugging.

Testing: Testing refers to the process of making sure that the program performs the intended task.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

1) What are the characteristics of a good programming language?

....

....

....

....

....

1.7 OPERATING SYSTEM

Operating System

1) An organized collection of software that controls the overall operation of a computer and supervises the execution of other programmes.

2) Software which controls the execution of computer programmes and which may provide scheduling, debugging, input/output control, accounting, compilation, storage assignment, data management and related services.

3) An integrated system of programmes which supervises the operation of the CPU, controls the input/output functions of the computer system, translates the programming languages into the machine languages and improves the total operating effectiveness of the computer.

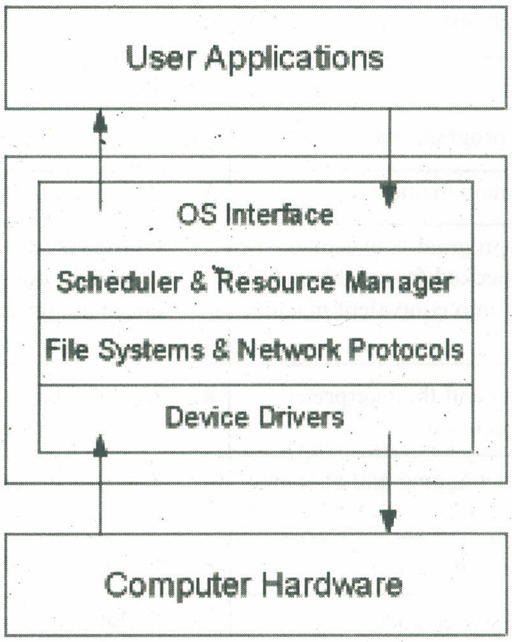


Fig. 8: Functions of operating system

Functions of operating system

Operating system acts as a resource manager because it controls all the parts of computer. How much memory is needed for the program? Where to store the program in which file and where to store the file in which place i.e. memory location and what are the devices are required to get the work done and which processor is required to complete the job all the operations are controlled by the operating system that is why operating system will act a Resource Manager.

There are four important managements of Operating system:

1) **Memory management:** The programmes in an operating system are capable of determining how much usable RAM a microcomputer has. The Operating system also decides how this RAM is used. The transferring or swapping of programmes and Data into and out of RAM takes place automatically under the control of the operating system.

2) **File management:** This will solve the problem of storing files separately from the computer and thus making retrieval a more straightforward operation and to allow two or more users to share the same file. The operating system supports a large library of user programmes and files. The user will only tell the name of the file. The operating system will determine where a file is and place that file in the secondary storage for use.

3) **Process management:** In processor management the processor is provided to the jobs for processing of jobs. It controls data transfers between memories, terminals, etc. It deals with error handling also. It controls the equipment also in synchronization.

4) **Device management:** It keeps track of all the Devices which device is required by the user and that device is given priority is allocated to the user for work. The operating system also closely manages the input output sub systems of the computer. Further, there are also several differences in the operational speeds of the processor and the speeds of the input-output devices which calls for buffering and blocking of each file which the operating system takes care of.

The facilities given by the Operating System are:

1) It initially set up the machine for operation-checking that the hardware is properly functioning.

2) It checks the opening and closing of files.

3) It assigns files to peripherals.

4) It controls read write activities.

5) It allocates the main and backing storage for program instruction, data.

6) It checks the error.

7) It handles the interrupts caused by program abnormalities.

8) It copies files from one disk to another.

9) It formats and prepare a brand new disk for use.

Types of operating system

1) **Single Program Operating System:** A single user operating system permits only one program to be run at a time.

2) **Multi-programming Operating System:** It is a method of executing two or more programmes concurrently using the same computer.

3) **Multi-tasking Operating System:** It is the performance of more than one task concurrently by one user on a computer system.

4) **Multi-user Operating system:** It manages the computer resources in such a manner that a number of users can use those resources at the same time.

5) **Multi-processing operating system:** In this environment operating system ensures that independent programmes are processed at the same time by different CPUs.

6) **Virtual Storage Operating System:** It is used for programmes that are too large to be contained within primary storage. The operating system permits data to be moved between primary and secondary storage.

7) **Virtual machine Operating System:** The virtual machine operating system gives the impression to each of a number of users that each has control over the computer while in reality they are sharing the same resource.

8) **Distributed Operating system:** A distributed operating system appears to its users as a centralized operating system for a single machine but it runs on multiple independent computers.

9) **Network Operating System:** It allows uses to access various network resources and controls access so that only the users with proper authorization are allowed to access particular resources. It provides network security features such as authentication, authorization, logon restrictions and access controls.

Commonly used operating systems

1) **MS-DOS:** It is developed by Microsoft Inc in 1981, is the most widely used operating system of IBM-Compatibles microcomputers.

2) **PC-DOS:** It is same as MS-DOS but developed by IBM for its personal computers.

3) **OS/2:** A multi-user, operating system developed jointly by IBM and Microsoft provides a unique feature of multi-tasking, where several programmes can be run simultaneously. It was the first operating system that provides users with a Graphical User Interface (GUI).

4) **Windows NT:** It is a multiuser 32 bit multi-tasking operating system for microcomputers and workstations developed by Microsoft Inc. It was driven by a need to exploit the tremendous power of 32-bit microprocessor.

5) **UNIX:** Initially developed by AT&T at Bell Laboratories in 1969, it is a highly successful operating system for powerful microcomputers, workstations and minicomputers, supports multitasking, multiuser processing and networking.

6) **Windows 3.x.:** To meet the need for an operating system that had a graphical user interface, Microsoft developed Windows, Windows 3.x refers to three early versions of Microsoft windows: Windows 3.0, Windows 3.1 and Windows 3.11. These windows versions were not operating systems instead they were operating environment. An operating environment is a graphical user Interface that works in combination with an operating system.

7) **Windows 95:** Microsoft developed a true multitasking system named Windows 95 also referred as Win 95. It is not like early versions of Windows which were merely operating environment.

8) **Windows 98:** Microsoft developed an upgrade to the Windows 95 operating system, called Windows 98. It is also called Win98 and is more integrated with the Internet.

9) **Windows NT:** It is an OS for high-end desktops and workstations. It is a 32 bit OS it is more powerful OS for Pentium range of processors.

10) **Windows 2000:** It is an upgrade to the Windows 98 and Windows NT operating System. It is complete multitasking operating system that has a graphical user interface.

11) **UNIX:** It is developed by Ken Thomson in 1970 for Bell laboratories. It supports a very strong security system by assigning each user a login name and a password. It provides a simple, uniform interface to peripheral devices. It has got built in networking with a large number of programmes and utilities.

12) **Linux:** It is a powerful version of the UNIX OS and is completely free of cost. It offers multi-tasking, virtual memory management and TCP/IP networking.

13) **Java Operating System (JavaOS):** Sun's JavaOS executes programmes written in the Java language without the need of a OS. It is designed for Internet and Intranet applications and embedded devices.

Check Your Progress 3

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is an Operating System? Explain.

....

....

....

....

2) Explain the difference between Linux and Unix Operating System.

....

....

....

....

1.8 COMPUTER NETWORKS

It is a collection of computers and peripheral devices connected together by communication links that allow the network components to work together. It is the act of process of informally sharing information and support, especially among members of a professional group.

Data Communication: It includes physical transmission circuits and networks and the hardware and software which support the data communication functions. It includes procedures for detecting and recovering from errors and contains the rules and protocols for exchange of information.

Features of Networking

1) It helps in sharing of computer resources.
2) It helps in sharing of software.
3) It helps in communication among users of different computer systems.
4) It facilitates communication with e-mail.
5) It allows decentralization of various data processing functions.
6) It reduces the cost of the system.
7) Network helps in sharing of work.
8) It makes the system reliable and available OnLine.

Network Topologies

Topology: It refers to the way in which communication network elements are physically connected to each other.

1) **Star Topology:** In star network no two computers can communicate with each other directly, the communication between them has to take place through the Host computer. In Star network there is a host computer and all other computers are connected to it.

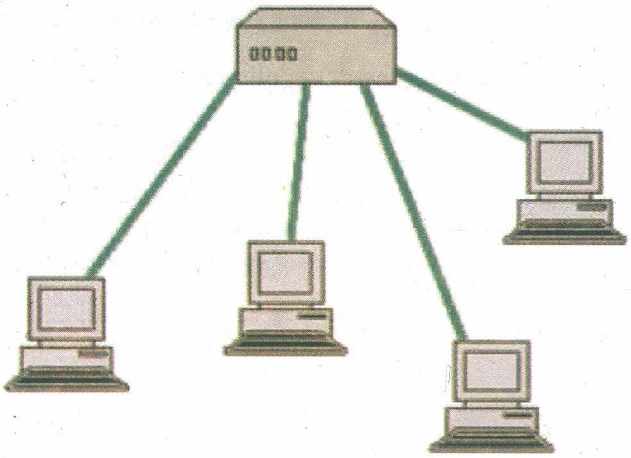


Fig. 9: Star Topology

2) **Ring Network:** No host computer exists in a ring network. All computers are connected in a ring form by a closed loop in a manner that passes data from one computer to another. There is a direct point to point link between two neighbouring or adjacent computers. These links are unidirectional which ensures that transmission by a node traverses the whole ring and comes back to the node, which made the transmission.

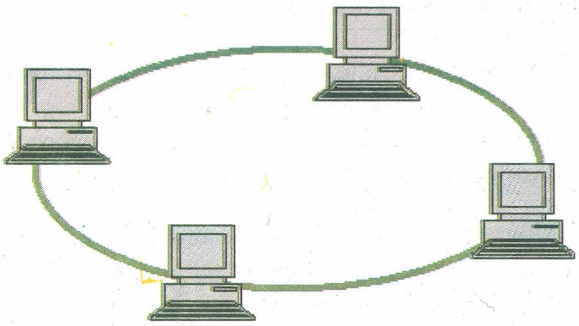


Fig. 10: Ring Topology

3) **Bus Network:** In this structure a single network cable runs in the building or campus and all nodes are linked along with this communication line with two end points called the Bus.

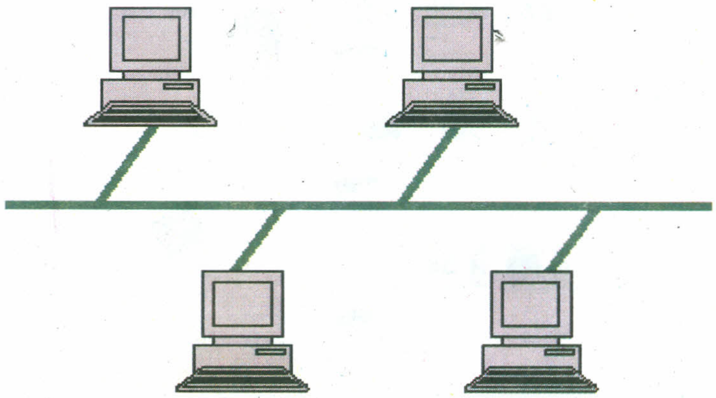


Fig. 11: Bus Topology

4) **Mesh Topology:** A mesh topology provides redundant communication paths between some or all devices

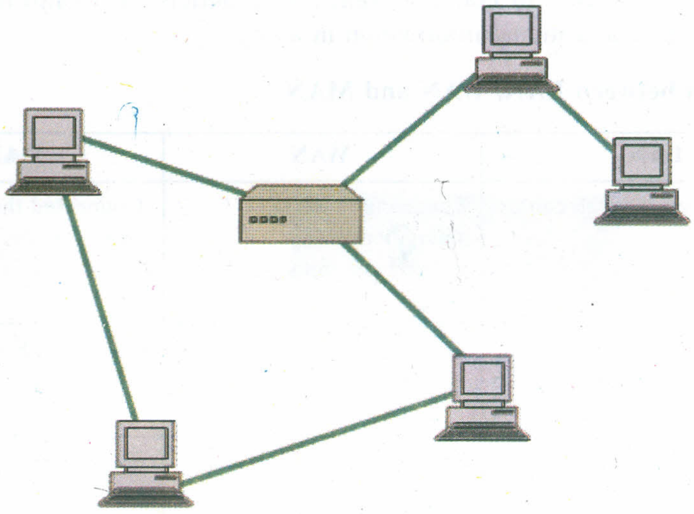


Fig. 12: Mesh Topology

5) **Tree Network Topology:** A tree topology integrates the star and Bus topologies in a hybrid approach to improve network scalability.

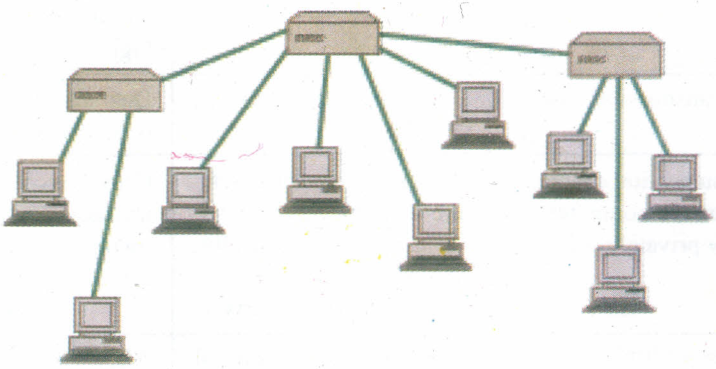


Fig. 13: Tree Topology

Local Area Network (LAN) – Networks used to interconnect computers in a single room, in a building or building in one site are called Local Area Network.

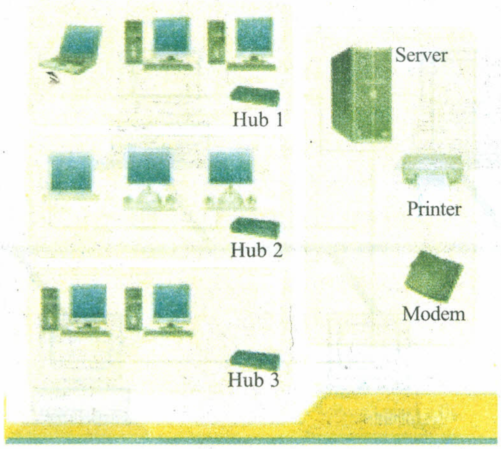


Fig. 14

Wide Area Network (WAN) – It is used to describe a computer network spanning a regional, national or global area.

Metropolitan Area Network (MAN) – it refers to a network confine to a metropolitan. It is used to connect branches or outlets of organizations or to exchange inter-organizational information in a city.

Comparison between LAN, WAN and MAN

LAN	WAN	MAN
1) Connected through cables	Connected through telephone lines, microwave links, satellite links	Connected through cables or telephone lines
2) Restricted to a small area in the same building or on the same campus	Works nationwide or even world wide	Located within the city
3) Symmetric topologies like bus, star and ring	Irregular topologies like mesh topology	Symmetric topologies
4) Easy installation	Difficult installation	Easy to install than WAN
5) Fewer data transmission error occur	Huge data transmission error occur	Not much data transmission error can occur
6) Data transmission speed is high	Data transmission speed is low	Data transmission speed is moderately high
7) Data transmission cost is low	Data transmission cost is very high	Data transmission cost is moderate
8) Communication channels between the computers are usually privately owned	Communication channels like long distance telephone service, satellite transmission etc. are provided by third party	Communication channels are privately owned as well as provided by third party
9) Enables multiple users to share software, data devices and physical media	Does not allow sharing of resources	Allows sharing of resources in a limited way

1.9 DATA TRANSMISSION MODES

There are three modes of data transmission:

1) Simplex mode
2) Half duplex mode
3) Full duplex mode

1) **Simplex mode:** Simplex communication is a simple method of communication in which there is one way of communication e.g. television transmission.

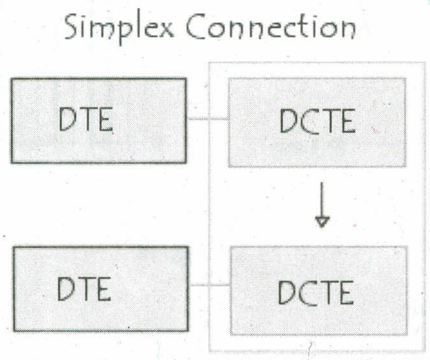


Fig. 15: Simplex Mode

2) **Half duplex mode:** In this mode both units communicate over the same medium but only one can use the line at a time while one is in send mode the other unit is in receive mode. It is like two persons talking to each other. One talks, the other listens. But neither one talks at the same time.

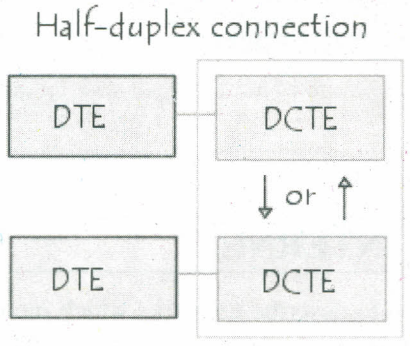


Fig. 16: Half duplex Mode

3) **Full duplex mode:** Fullsx duplex system permits information to flow simultaneously in both directions on the transmission path.

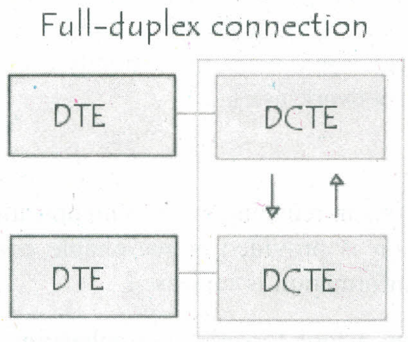


Fig. 17: Full duplex Mode

Analog and Digital Data transmission

Analog Data Transmission: Sound coming out from an instrument is an Analog Data communication. Analog Data is continuous over an interval.

Digital Data Transmission: Digital data is discrete. They have to be represented by a sequence of bits for communication for example text and integers.

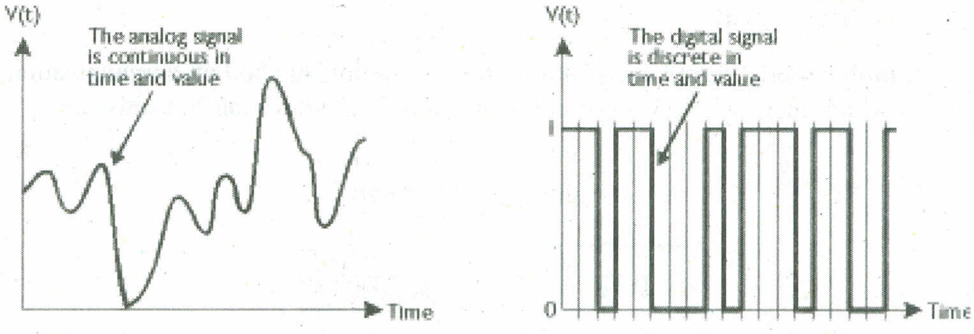


Fig. (a): Analog **Fig. (b): Digital**

Fig. 18

Check Your Progress 4

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of this Unit.

1) What is computer network? Explain with the help of examples.

....

....

....

....

....

1.10 WHAT IS INTERNET?

The word Internet is used to describe networks which incorporate a very large and complicated set of equipment. A set of computer networks made up of a large number of smaller networks using different networking protocols is called Internet.

The Internet, the network is a globe spanning heterogeneous mix of technologies and operating systems.

The Internet is a global collection of high powered computers that are connected to each other with network cables, telephone cables, microwave dishes, satellites and very other kind of electronic wizardry currently available facilitating several information services for network users.

Benefits of internet

Internet helps organizations in reducing their communication costs significantly as access to the information is provided at reasonable cost. Employee access to significant amounts of information is increased.

The Internet has become a tool for effective enhancing of communication and coordinating activities in far flung locations. Internet provides an efficient means of updating and disseminating current information to customers and internal staff of organization.

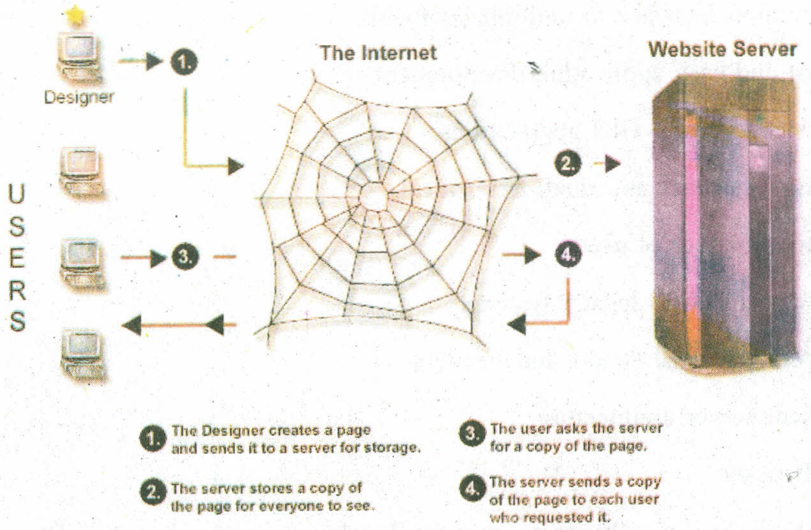


Fig. 19

Internet recruiting is very popular in the present age of talent war throughout the world today which involves advertisement of vacancies on the Internet and getting applications from the intending candidates through the Internet.

Internet has provided opportunity to organizations and their customers for interactive dialogues on direct marketing of products and services. Using Internet, the students can get information on different institutions of higher education in any part of the world.

Service provided by the Internet

E-mail – It permits the sending and receiving of messages to other users connected to the Internet.

FTP (File Transfer Protocol) – It means of sending and receiving files from one computer to another..

GOPHER – An early form of representing information as Graphical Icons or Symbols that could be displayed in a window and then downloaded. It has been replaced by www.

USNET – A number of discussion groups that allow users to post questions and replies sorted by topic.

WWW (World Wide Web) – Accessed using a web browser such as Interne Explorer, Netscape Navigator, a means of locating and displaying information located on the Internet.

WEB

The web refers to a specific kind of Internet Interface. The web documents contain links that lead to other web pages. The web made it possible for novices to use the Internet.

Features of WWW

1) Platform independent

2) Global availability

3) Distributed computing

4) Hypermedia support

5) Common interface to multiple protocols

6) Fast and easy application development

7) Easier to create GUI applications

8) Easy and quick information retrieval

9) Large number of users

10) Integration with legacy systems

11) Opens standard vendor independent

12) Client server architecture

Web Browser

A web browser is a software programme developed to provide a friendly interface on the web. It displays the web page and moves between the websites. It plays an important role in managing interaction with the web and also helps to review web contents.

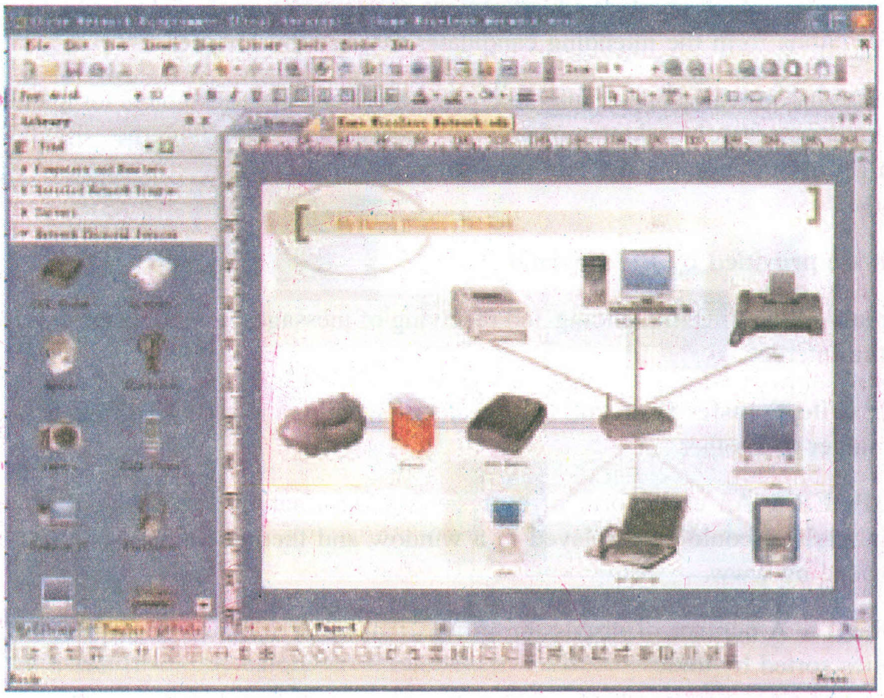


Fig. 20

Functions of Browser

1) Interface on the web

2) Display web page

3) Interaction with web

4) Review web content

5) Download, save, copy or print the web page

6) Maintains record of history of sites last visited

Uniform Resource Locator (URL)

These are used to address and access individual web pages Internet resources. The format of a URL is: Protocol/Inter Address/Web page address. For example http://www.khoj.com, http://www.google.co.in

http	:	identifies the site as on the world wide web using HTML, of hypertext markup language
://	:	the actual URL, which is broken up by the periods
www	:	identifies the site as part of the world wide web. The web is the subset of the Internet
net	:	is the top level domain name. It indicates the purpose of the sponsors of the site
.com	:	commercial organizations. This domain in intended for commercial entities i.e companies
.edu	:	educational organizations. This domain was originally intended for educational institutions
.mil	:	military purposes
.gov	:	government organization. This domain was originally intended for any kind of govt. office
.org	:	general organization. This domain is intended as the miscellaneous top level domains for organizations that did not fit anywhere else. Some non govt. organizations may fit here
.net	:	this domain is intended to hold only the computers of network providers i.e. the NIC and NOC computers
.int	:	this domain is for organizations established by international treaties or international databases.

1.11 INTRANET

The Intranet is a type of information system that facilitates communication within the organization, among widely dispersed departments, divisions and regional locations. Intranet connects people together with Internet technology using web browsers, web servers and data ware houses in a single view. Within an Intranet, access to all information, applications and data can be made available through the same browser.

1.12 EXTRANET

An Extranet is private network that uses the Internet protocol and the public telecommunication system to securely share part of a business information or operations with suppliers, vendors, partners, customers. An Extranet can be an extension of an Intranet that makes the latter accessible to outside companies with an Intranet. Extranets provides the privacy and security of an Intranet while retaining the global reach of the Internet.

1.13 COMPUTER SECURITY

Three types of securities may be provided to the computer:

1) Hardware security

2) Software Security and

3) Information Security

1) **Hardware Security** – the hardware security is achieved by ensuring control on entry to the computer centre, by providing uninterrupted power supplies hardware insurance etc. physical security is achieved by provision of locking arrangement.

   - It comprises arrangements for fire detection and fire avoidance, pollution damage and unauthorized intrusion on computer equipments.
   - A dust free environment in the computer room is a must.
   - Cover hardware with protective fabric when it is not in use.

2) **Software Security** – Software security is provided by using original software for operating system, compilers or software packages.

   - Use correct procedures for shutting down the computer so that all the files would be properly closed.
   - Keep back-ups of all the files.
   - If one develop his/her own applications, introduce passwords to access the application.

3) **Information Security** – The protection of the interests of those relying on information and the information systems and communications that delivers the information, from harm resulting from failures of availability, confidentiality and integrity.

   - Responsibility and accountability must be explicit.
   - Awareness of risks and security initiatives must be disseminated.
   - Security must be cost-effective.
   - Securities must be addressed taking into considerations both technologies and non-technological issues.
   - Security must be coordinated and integrated.
   - Security must be reassessed periodically.
   - Security procedures must provide for monitoring and timely response.
   - Ethics must be promoted by respecting the rights and interests of others.

1.14 VIRUS

A virus is a programme which reproduces its own code by attaching itself to other programmes in such a way that the virus code is executed when the infected programme is executed. The virus does this without the permission or knowledge of the user.

Computer Virus

Computer viruses are the class of programmes that reside in the storage media of computer and infect other programmes which work well and replicate/multiply themselves in the computer without the user's knowledge.

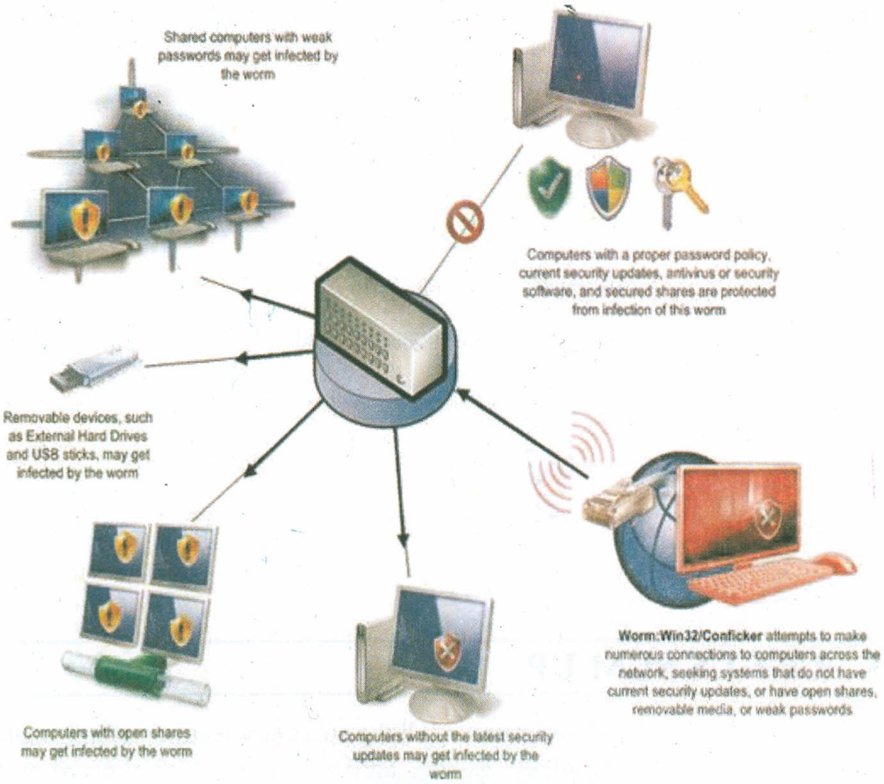


Fig. 21

Symptoms of Virus Attack

- Less system memory than the actually installed memory.
- Hanging up of machine and programme for no particular reasons.
- Hampering functions of I/O devices.
- Slowing down of execution system.
- Abnormal screen display.
- Delayed disk operations.

Protection from Viruses

- **Use of Antivirus software** – Antivirus software is special software designed to check comp uter systems and disks for the presence of various computer viruses.
- **Procurement of Software from reliable Sources** – It is better to procure the software from reliable sources in its original form with factory sealed packages.
- **Testing New Applications on Stand-alone System** – When a new application is developed, it is better to test it on stand-alone system before the application is used on computer network.
- **Educating the users and computer operators** about the possible threats from viruses, taking special care on the day and time of virus attack.

Check your Progress 5

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Define Information Security. Write the various principles of information security.

....

....

....

....

2) What is Virus? What kind of protection can be used to overcome virus problem?

....

....

....

....

1.15 LET US SUM UP

This unit covers the detailed descriptions of all the necessary features of information technology. Information technology, usually abbreviated as IT, is defined as the umbrella covering all activities associated with computer based information systems. It is defined as the study, design, development, implementation, support or management of computer based information systems. This unit actually deals with how to use computer software and hardware and computer networks to produce, store, protect, process, transmit and retrieve securely and efficiently the information.

1.16 CHECK YOUR PROGRESS : THE KEY

Check Your Progress 1

1) A computer is a high speed, general purpose, digital electronic, stored programme data processor, i.e. Computer is an electronic machine that performs a specified sequence of operations as per the set of instructions (programmes) given a set of data (input) to generate desired information (output).

   The classification of computers is based on the following three criteria: According to purpose, According to technology used, According to size and capacity

2) RAM (Random Access Memory): It is a temporary memory and it is used when the programme and application is in execution process. RAM is volatile.

   ROM (Read Only Memory): It is a permanent memory and can only be read; data cannot be written into it. ROM is permanent and non-volatile.

Check Your Progress 2

1) A good programmeming language should be easy to understand.

   The structure of the language should be very simple and it should have a very simple syntax.

It should have availability of appropriate data structure so that solving a given problem may be quiet easy.

It should have presence of appropriate support environment and functions such as editors and extra library functions.

It should be easy to verify and modify thus reducing the programme development time and increase the efficiency of the resultant software.

Check Your Progress 3

1) Operating system is an organized collection of software that controls the overall operation of a computer and supervises the execution of other programmes. Software which controls the execution of computer programmes and which may provide scheduling, debugging, input/output control, accounting, compilation, storage assignment, data management and related services.

   An integrated system of programmes which supervises the operation of the CPU, controls the input/output functions of the computer system, translates the programmeming languages into the machine languages and improves the total operating effectiveness of the computer.

2) **UNIX** – It is developed by Ken Thomson in 1970 for Bell laboratories. It supports a very strong security system by assigning each user a login name and a password. It provides a simple, uniform interface to peripheral devices. It has got built in networking with a large number of programmes and utilities.

   Linux – It is a powerful version of the UNIX OS and is completely free of cost. It offers multi-tasking, virtual memory management and TCP/IP networking.

Check Your Progress 4

1) It is a collection of computers and peripheral devices connected together by communication links that allow the network components to work together. It is the act of process of informally sharing information and support, especially among members of a professional group.

Check Your Progress 5

1) The protection of the interests of those relying on information and the information systems and communications that delivers the information, from harm resulting from failures of availability, confidentiality and integrity.

   - Responsibility and accountability must be explicit.
   - Awareness of risks and security initiatives must be disseminated.
   - Security must be cost-effective.
   - Securities must be addressed taking into considerations both technologies and non-technological issues.
   - Security must be coordinated and integrated.
   - Security must be reassessed periodically.
   - Security procedures must provide for monitoring and timely response.
   - Ethics must be promoted by respecting the rights and interests of others.

2) A virus is a programme which reproduces its own code by attaching itself to other programmes in such a way that the virus code is executed when the infected programme is executed. The virus does this without the permission or knowledge of the user.

Protection from Viruses

- Use of Antivirus software – Antivirus software is special software designed to check computer systems and disks for the presence of various computer viruses.
- Procurement of Software from reliable Sources – It is better to procure the software from reliable sources in its original form with factory sealed packages.
- Testing New Applications on Stand-alone System – When a new application is developed, it is better to test it on stand-alone system before the application is used on computer network.
- Educating the users and computer operators about the possible threats from viruses, taking special care on the day and time of virus attack.

1.17 SUGGESTED READINGS

- Computer Networks by S.K. Yadav.
- Computers and information technology by V.K Kapoor.
- Fundamental of Information Technology By Alexis Leon and Mathews Leon.
- Information Technology by Vishnu Priya Singh and Meenakshi Singh.
- www.microsoft.com/workshop/networking/cifs/default.asp.

UNIT 2 SECURITY AWARENESS

Structure

2.0 INTRODUCTION

Security: the state or quality of being secure; freedom from fear or danger; defense or protection.

Awareness: knowing, conscious, alert.

We use Computers practically for most of our jobs lives these days and hence are too much dependent on them. We use them as tools for work, data storage, schoolwork, shopping and entertainment. As a lot of important information is always stored on our computers we have to make sure they are protected from any kind of loss of information. Businesses also have to secure information on their computers to protect it from various forms of attacks day and night. The PC of an individual user is also not safe anymore as most of the PCs are part of a big network i.e. Internet and hence open to all kind of attacks from various sources.

A generic term is used to define all these risks and called "computer security risk." This term refers to the likelihood that some action could cause the loss of information, computer hardware or denial of service.

Although we can't expect all computer users to be technically sound to handle all the security related issues themselves, we can at least make them aware about the security issues and other impact factors that may be critical to the mission of an organisation.

The "Security Awareness" or "Information security Awareness" is an activity simply to focus attention on security. Awareness programmes are intended to allow individuals to recognise IT security concerns and respond accordingly. At the same time, we have to remember that "Security Awareness" is not training and we have no intention to train people to handle the eventualities rather we are making them aware of when to raise alarm and to whom.

2.1 OBJECTIVES

After studying this unit, you should be able to:

- understand the need of Security Awareness;
- explain different activities related to Security Awareness; and
- understand the roles played by different people in Security Awareness Programme.

2.2 FUNDAMENTALS OF SECURITY AWARENESS

"People are our greatest strength and our greatest weakness."

The saying summarises and empahsises the very need of Security awareness and explains us as to why security awareness is so important. All organisations have people using their IT systems. If these people are not aware or made aware of how to properly use the systems and taught about potential attacks and scams, it can't be guaranteed that our systems will remain protected and used securely.

It is important that both home and business computer users take action to shield their computer from these threats to their security. Computer security methods are not always 100% foolproof but they have the capacity to decrease the risk to computers significantly. As soon as a solution is found to protect against one threat, a new way to gain unauthorised access to them is invented. Computer users on home networks are more at risk to have information stolen than are computers on business networks mostly because of the more advanced security on the latter. And the internet is a network even more susceptible and at risk when it comes to security. Another problem with security on the internet is that there is not one centralised point to manage security and safety on the information highway.

Security awareness is an important element of protective security. Awareness provides physical, information and personnel security measures as well as informing staff of their governance requirements such as rights, duties, ethics etc.

As we have stated earlier that awareness is not training. However, some people tend to mix training with awareness.

The basic objective of awareness is to change the behavior of a user, administrator or owner of a system to that of a more secure behavior. The basic objective of training is to give the user, administrator or owner of a system the necessary skills to securely use that system.

It should be generally made mandatory for every user/employees to undertake security awareness as soon as possible after starting with the company. It is also a good idea for companies to include security awareness in their induction programmes.

Companies should hold regular awareness sessions to confirm prior knowledge and inform employees of any new measures. Companies should hold additional sessions if the threat environment changes.

An example of a topic for an awareness session is virus protection. The subject can simply and briefly be addressed by describing what a virus is, what can happen if a virus infects a user's system, what the user should do to protect the system and what the user should do if an infection virus is discovered.

2.3 SECURITY AWARENESS PROGRAMME LIFE CYCLE

Managing Information system security is no mean task and a never ending effort. Irrespective of how well we secure a system today, new threats and issues will appear tomorrow that will send chills down our spine. User support, IT staff enthusiasm and management buy-in are critical assets for overcoming the constant barrage of threats.

It is because of the above reasons that Information security awareness must be made an integral part of any security plan or programme. Employees at all levels must be made understand that they have to play a large part in protecting the agency's information assets. Awareness teaches employees that they are a key piece of the total security environment. Through continuous awareness sessions, everyone will start taking "Security" as a matter of daily practice. Only with full support and cooperation of all employees and management can a successful Information Security Awareness Programme be established and maintained.

In this section, we discuss a four step life cycle of an Information security awareness programme:

Steps 1 : Awareness Programme Design

In this step, a company wide needs assessment is conducted and a training strategy is developed and approved. Every company has its own working domain and similarly threat domain. The analysis helps in determining on what issues should be discussed in detail and which issues should be left out of discussion. Strategy designed for one company may not fit for other one because of difference in working environment.

This strategic planning document identifies implementation tasks to be performed in support of established company security training goals.

Step 2 : Awareness Material Development

After the analysis and assessment of threats and categories is over, it is time for security officers to develop the materials to be used for training either in house or by outsourcing the same.

This step focuses on available training sources, scope, content and development of training material, including solicitation of contractor assistance if needed.

Step 3 : Awareness Programme Implementation

This is the most critical phase of the security awareness life cycle as it disturbs the whole schedule of the organisation. All the users need to be trained, but it is almost impossible to make all of them available for such activity putting at risk the productivity of the organisation. This step demands a lot of persuasion and adjustments both on the part of trainers as well as trainees.

This step addresses effective communication and roll out of the awareness and training programme. It also addresses options for delivery of awareness and training material (web-based, distance learning, video, on-site etc.).

Step 4 : Post-Implementation Activities

This phase is actual operational phase as the user is going to put to practice whatever he/she has learnt in earlier phase. It may cause some temporary disturbance, if the user is not properly trained or has misunderstood some concepts.

This step also gives guidance on keeping the programme current and monitoring its effectiveness. The security team has to constantly organise some activity like feedback methods (surveys, focus groups, benchmarking etc.) to keep the security aspects in focus. We will discuss more on this in further sections.

Models used for Security Awareness Programme

The Security awareness life cycle can be implemented using any of the following three common models

- **Centralised Model**

  All responsibility resides with a central authority (e.g. Chief Information Officer (CIO) and IT security programme manager). This model may work for a small organisation where number of users are limited or strict security guidelines are in place with mature users.

- **Partially Decentralised Model**

  Training policy and strategy lie with a central authority, but implementation responsibilities are distributed. This model is for those organisations, which are multi-locations or multi-department. The training for department or location in charges can be conducted at a centralised place. The trained persons can then take care of imparting training for users under their control.

- **Fully Decentralised Model**

  Only policy development resides with a central authority and all other responsibilities are delegated to individual company components. This model is suitable for large organisation as it takes care of formulating a uniform policy for all the regional offices to follow.

  Security awareness efforts are designed to change behavior or reinforce good security practices. Companies can supplement the security awareness efforts using any of the following simple methodologies:

  - By running campaigns that address the ongoing needs of the company and the specific needs of sensitive areas, activities or periods of time
  - By providing security instructions and reminders via publications, electronic bulletins and visual displays such as posters
  - By including protective security-related questions in staff selection interviews
  - Performing various mock drills and exercises
  - Inclusion of security attitudes and performance in the company performance management programme.

It is recommended that the programme should use a mixture of delivery methods and comprise of hands on tasks.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What is Information Security awareness?

....

....

....

....

2) What are the four step of life cycle of an Information security awareness programme?

....

....

....

....

3) What is the difference between partially decentralized model and fully decentralized model?

....

....

....

....

2.4 SECURITY AWARENESS SUBPROGRAMMES

An information security awareness programme brings Information security awareness to a personal level. Since everyone is responsible for the security of the information they use, it is important that they should be taught as to how to incorporate the rules and procedures into their daily operations. The idea here is to make security a part of everyone's day without being repetitive. But, every such awareness programme requires creativity and constant updation in pedagogy.

<table>
<tr><th colspan="4">Decision Table for users</th></tr>
<tr><td colspan="2" rowspan="2">Detection of suspicious activity/ problem</td><td colspan="2">Situation Critical?</td></tr>
<tr><td>Yes</td><td>No</td></tr>
<tr><td rowspan="2">High Importance</td><td>Yes</td><td>SOS Alert (through SMS/Phone)</td><td>Inform (email)</td></tr>
<tr><td>No</td><td>Post advisory instruction</td><td>RELAX!!!</td></tr>
</table>

Fig. 1: Decision Table used for training

The above table describes how a user should respond in case of any eventuality. This decision table should serve as a starting point of awareness programme.

An information security awareness programme process of a company consists of two major tasks:

1) Awareness Sessions

2) Awareness Materials

The purpose of this programme should be to provide structure to an awareness programme so that it can cover all the users. It may include training techniques, materials to produce and communication correspondence to announce, deliver and support the awareness programme.

2.4.1 Awareness Sessions

In the awareness sessions, all employees should be taught the importance of information security. They should be told explicitly about the rules that must be followed and what to do if there is a violation. This activity acts as a pillar to Information Security Awareness campaign in any organisation.

Information security policy and standards are rendered ineffective if individuals at any level of the company are unaware of the importance of security policy, do not understand established standards or fail to perform required practices for any reason. Good security is "a state of mind" that can best be achieved by a programme or process that reinforces the concern for protecting our information assets and appropriate actions for doing so on a regular and ongoing basis.

2.4.2 Awareness Materials

We must be clear that providing training about Information security is not a one-time event. Good security practices are never obvious, intuitive or easily incorporated into established routines. To improve the effectiveness of information security standards, they must be known, understood, believed to have value and appropriately and consistently practiced.

The awareness programme must be supplemented with a good material that the user may be allowed to have so that it can also be used for any future reference. The material may either be a simple text material or can be an adio/video tutorial. The materials provided must contain the company's position with regard to handling the many aspects of information security. All the rules, guidelines, do's and don't's should be properly elaborated in the materials.

Continuous and positive supplies in the form of new and innovative materials help improve the level of information security and strengthen the policy. Without such efforts, policies or standards may be perceived as not relevant, necessary or valuable and may be "followed" but not be practiced in a manner that supports full effectiveness.

The following tools can help us to keep our awareness programme meaningful:

- **Refresher campaign sessions**

  An awareness campaign is a good way to initially incorporate an information security awareness programme. A campaign can "advertise" that the information security awareness programme is coming soon and with good promotional items, the company can gain employee's attention, emphasise key points and even educate them on key security issues.

  i) Give small prizes (i.e. free lunch or a coffee cup) for exemplary staff.

  ii) Give "traffic ticket" warnings reflecting rule violations. (i.e. workstations not logged out or locked during a fire drill)

iii) Adopt an annual Information security awareness day with special educational materials and events.

iv) Use the "tagline" of "Focused on Security, Committed to Success" as the theme that represents Information security awareness at our company such as.

- **Regular updates to materials**

Every organisation needs standardised information security awareness programme materials. It may also need to develop additional training materials, checklists etc. as and when company's needs change and evolve.

At staff meetings or group meetings, handouts about awareness issues are a great way to get tips into users' hands and in front of them in a non-computer based manner. A handout can include a small pamphlet explaining why it is important to use secure passwords, the latest information on identity theft or how to catch a phishing scam.

Promotional items, similar to handouts, can include items such as a small desk calendar that, for each month, gives a different awareness tip; a planner that gives reminders to reset passwords on days to match password policies; or a stress doll that represents a sick computer, which a user can squeeze. These items are great things to hand out because the users can place them on their desks, see them everyday and become more aware.

- **Top management communications to staff**

Sending weekly or monthly e-mails from top management is a great way to keep your community up-to-date on the latest tips and remind them about the old tips that they might have forgotten. It is also a great way to give them real-world examples of what happens if security is breached. For instance, you could send out an e-mail that references a recent laptop that was stolen and had saved on it thousands of records of people's social security numbers and addresses. Use examples like this to help reinforce what you want to show them to help change their behavior.

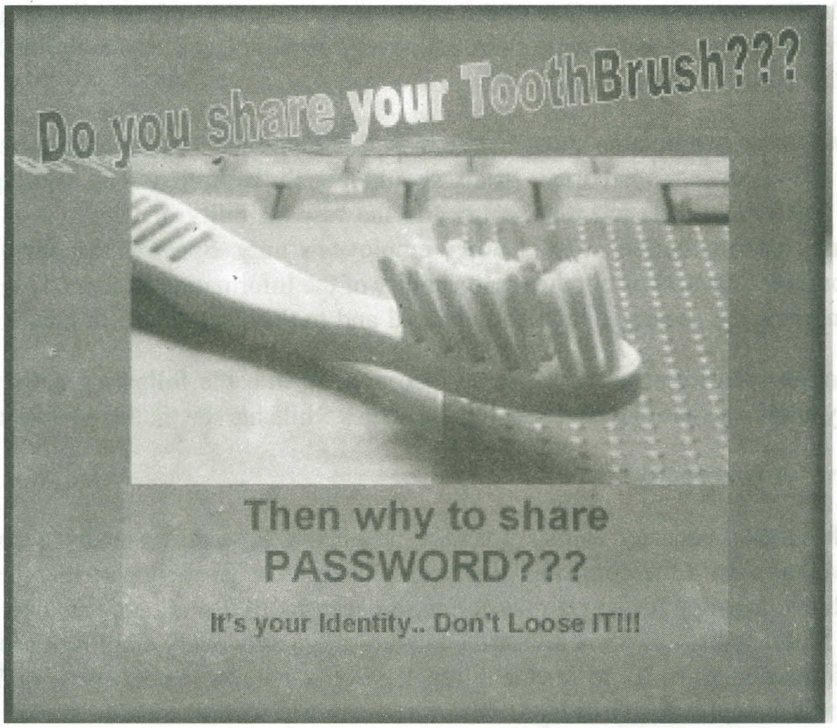


Fig. 2: A model poster depicting importance of Password

The management may use any of the following tools to send their message across to their staff:

- E-mail messages
- Articles in the company's newsletter
- Magazines, internet articles for circulation
- Bulletins and alerts
- Posters
- Web announcements
- Quiz (to measure results of the programme)
- Giveaways – buttons, pens, certificates, t-shirt's, mouse pads, pen holders, coffee cups

An organisation can leverage web sites loaded with awareness information to get the latest awareness information to the community. These sites can give the users a place to check for policies; contact information if they think a security-related incident has occurred; a list of security personnel and contacts; links to other awareness sites; and tips on how to secure their computers at home, because they were likely to have not been the ones to secure their own computers at work.

It has to be kept in mind that an activity such as awareness programme cannot be conducted in a vacuum. It will surely eat a lot of productive man-hours of an organisation, therefore it is imperative for the management to strike a balance among the productive and safeguard activities so that the organisation is not negatively impacted on account of security awareness programme.

2.5 MAKE SECURITY AWARENESS IMPLICIT

Every organisation has its own set of activities that every employee has to undergo e.g. induction, interview etc. One of the easiest ways to implement a quality security policy in organisation is to incorporate it in every possible activity thereby making it implicit.

The awareness programme must begin with the support of senior management. Ideally the Head or the Security Officer should launch the initiative by sending an e-mail briefly summarising that security is the responsibility of everyone in the company. Information security is every employee's duty. Specific responsibility for information security is not the responsibility of the Information Systems Division only. Information security is multi-divisional and multi-disciplinary in nature.

Information security awareness can be incorporated into the following activities, as every employee has to pass through these stages while his stay in the organisation.

1) **Involve everybody**

   Information security cannot possibly be adequately addressed by a single division within the company. Every employee must do their part in order to achieve appropriate levels of information security. After all, information can be found nearly everywhere in the company and nearly every employee utilises information in order to do their job. It is only natural that every employee should be specifically charged with responsibility for information security.

2) **Continuous awareness refresher courses**

All employees (employees, consultants, contractors, temporaries etc.) must receive some level of information security awareness and training. This training requirement must be included in all contracts. Workers must be provided with sufficient training and supporting reference materials to allow them to properly protect the company's information assets. Management should allocate sufficient on-the-job time for employees to acquaint themselves with the company's security rules, procedures and related ways of doing business.

3) **New Performance review orientation**

The company should go one step further and incorporate a question into performance review forms. The question could read something like this: "Does the employee observe information security policies in the course of his/her work?" It must also be supplemented with additional instructions, telling employees exactly what is expected of them.

Employees failing in such reviews should be motivated top take up the security policies more seriously. At the same time, employees getting good grades in these assessments should be suitable rewarded.

4) **Don't Exclude Contractors and part timers**

Contractors, agents working on behalf of the third party, auditors and other nonemployees in a position to impact the security or integrity of information assets of the company will be made aware of the appropriate Information Security Policies. These individuals must sign a statement acknowledging they have received and read the policies and understand their responsibilities in addition to signing a Non Discloser Agreement.

5) **Mandatory Awareness Training**

Information security awareness training must be made mandatory. Every employee must attend an information security awareness class soon after the date of employment. To provide evidence that every employee has attended such a class, each employee must sign a statement that they have attended a class, understood the material presented and had an opportunity to ask questions.

6) **Signed Agreements**

Without confirmation that all new and existing employees are aware of security policy there is no assurance that the desired actions are understood or followed. Failure to follow security policy or practice security standards for any reason reduces the value of such statements to "documents of prosecution" and negates the positive reinforcement and protective intent for which the information policy and standards exist.

The company should require users to sign a statement that they agree to:

- Abide by information security policies and procedures. A signature on a form with this statement and a summary of the policies and procedures, can be required before a user is given a user-ID and a password.
- Their understanding of the security policy by annually signing a form acknowledging that they agree to subscribe to security policy. The intention is to annually remind employees that they must abide by the company's security policy. From a legal standpoint, it is desirable to have employees acknowledge in writing that they have read and understand that adherence

to these policies is a required part of their job. If they are subsequently terminated due to security policy related problems, there is no doubt that the employee understood what was required of him or her. This agreement therefore reduces the probability of a wrongful termination lawsuit.

- To provide evidence that every employee has attended mandatory information security awareness class, each employee must sign a statement that they have attended a class, understood the material presented and had an opportunity to ask questions. For existing employees, a modification of this agreement could state they must attend within six months of the date when such courses become available.
- Every worker must agree in writing to perform his or her work according to security policy and procedures.
- All employees with access to computer systems must be informed of security policies and procedures and their responsibilities in writing. All new employees will sign a statement acknowledging they have received and read the policy and understand their responsibilities. This should include knowledge of the consequences of violations of security procedures.
- A signed statement indicating awareness, compliance and intent of continued compliance with information security policy and standards will be required upon annual review of each employee.

Check Your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) What major tasks are performed by information security awareness programme process of a company?

....

....

....

....

2) Explain Awareness Sessions.

....

....

....

....

3) What tools may be used by the management to send their message across to their staff?

....

....

....

....

4) Explain Continuous awareness refresher courses.

....

....

....

....

2.6 MANAGEMENT AND LEVELS OF AWARENESS PROGRAMME

It should be understood that not all level of personnel require same level of security awareness. Managers at any level many require a different view of information security business practices. Upper level management may need simply an executive overview, while middle management and user management may need to know more about prevention, detection and incident reporting.

2.6.1 Management of Awareness Programme

The organisation needs to run different kind of awareness programme for different set of users. It has to be managed via various tailor-made programmes and can be classified as following:

1) **For Permanent staff**

   Security awareness training for permanent staff is a must but it is very difficult to stop regular work of the company and invite the staff for training. It is generally implemented by extending the office hours or taking the staff on an outdoor picnic for training sessions.

   The participants are mainly the computer users and in charge of important data entry, analysis etc. The largest of all audiences, permanent staff requires a unique awareness programme tailor made for them.

2) **For Temporary staff**

   The awareness training for this group may be conducted on ad-hoc basis. They may be called in small groups over the weekend or during lean period.

   The temporary staff may not need as much training as the permanent staff since HR issues and such may not apply. They are not necessarily a separate audience, but are a subset of the computer user.

3) **Contractors, Agents, Auditors and Non-employees**

   This group is likely to be the most defaulter of the lot that will not follow the security policy because of ignorance. It is in the interest of the company to train this group to make sure that the security is not compromised on any account.

   This group may be clubbed with temporary staff and provided with the basic training.

4) **Technical Staff/Management**

   This is a highly specialised and separate audience from the Permanent Staff group. They require a unique training class. Although, it should be preferred that they also attend the permanent staff programme.

This group must also be provided enough skills to handle the emergency situations. They should also be groomed as future trainers so that regular awareness activities are handled by them.

5) **Security Officer/Staff**

The division security officers and security administrator staff is a separate audience and they require a unique training class. Apart from technical expertise, they also need managerial acumen to handle the staff under them.

2.6.2 Level of Awareness Programme

Not all people face all the problems. As the responsibilities of persons differ according to their role, their reporting and handling of the problem needs to be different. The level of security awareness and training should be commensurate with the level of access and expertise required in relation to the system components and information resources for which the employee is responsible.

- Security awareness and training should be incorporated for all new hired employees.
- All employees should receive security training prior to being provided any access to IT systems and resources. Prior to accessing any specific software applications, employees should receive specialised security training as appropriate focused for their role and responsibility relative to the software application system.
- The receipt of security awareness training should be documented in the employee's personnel file with the employee's acknowledgement of having received and understood the training.
- Security awareness shall be promoted on an on-going basis. The employees should have their security awareness training updated annually or upon occurrence of a specific event, such as a change in job responsibilities, employment status etc.

2.7 BASIC SECURITY THREATS AND HANDLING GUIDELINES

In this section, we discuss basic threats that a computer user may face. We also suggest some basic guidelines that must form core of any security awareness programme so that the users may become educated and informed to gauge the level of threat in order to be able to take further corrective measures.

Security Threats

1) **Viruses, Worms and their handling**

Viruses are computer programmes that are designed to spread themselves from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer or slowly infect the documents on that computer, but it does not intentionally try to spread itself from that computer to other computers. In most cases, that's where humans come in. We send e-mail document attachments, trade programmes on pen drives or copy files to file servers. When the next unsuspecting user receives the infected file or disk, they spread the virus to their computer and so on.

Worms, on the other hand rely less upon human behavior in order to spread themselves from one computer to others. The computer worm is a program that is designed to copy itself from one computer to another over a network (mostly by using e-mail). The worm spreads itself to many computers over a network and doesn't wait for a human being to help. This means that computer worms spread much more rapidly than computer viruses. It eats a lot of network bandwidth while spreading and slows down the network.

How to handle/avoid Viruses and Worms

i) A user should make sure that the system has a good anti-virus programme installed on it. If the anti-virus is not available, the demand for the same must be raised immediately.

ii) While sending/receiving e-mails, attachments should be avoided. The content of the file should be sent as a body of the e-mail rather than as an attachment.

iii) Don't click links in e-mail unless you are absolutely sure you know the sender and recognise the URL.

iv) Do not open/download an attachment/file unless you trust the source.

  a) Do you know the person who is sending you this file? E-mail addresses can be "spoofed" – the "from" address can be faked.

  b) Does it make sense that they are sending it to you?

  c) Microsoft NEVER sends operating system patches as e-mail attachments. They will ask you to visit the Microsoft Web site to download any software.

  d) If you're not sure, ask the sender to resend the attachment to verify that they actually sent it to you.

  e) Do not enter personal information into any web site form unless you are certain:

  - That the web site is authentic – clicking on a link in an e-mail can send you to any web site, make sure you are in the right place.
  - That the web site is secure – the lock icon in the bottom right corner of your browser will display as closed and highlighted.

Action to be taken in case of infection

i) Contact the Helpdesk of your organisation.

ii) Remove your machine from the network to stop the spread of infection.

iii) Wait for help to arrive.

2) **Passwords**

Although, it may sound as absurd that the password may be a security threat, it is true that a bad password is as much a security threat as having no password.

A password is a unique alphanumeric combination provided to a user or machine to prove that only the legitimate users use the systems for legitimate purposes. The user should make sure that the password has enough degree of complexity so as to make it difficult if not impossible to guess the same.

A simple password may be guessed easily and the security can be compromised using guessed password. Sharing of password is another activity that most of the computer users do as they trust their colleagues. This can prove disastrous as more than 80% of system break-ins are performed not by outsiders, but by insiders.

Guidelines relating to Passwords

i) A password should be generally consisting of 8 characters or more, not a word, mixed case, mixed characters. Do not use your name or the name of a family member, your pets name, your favorite past time or sports team. These are easily guessed!

ii) You should never share your password for the reason that the onus of any activity, legal or illegal, performed by using your password lies with you.

iii) You should never save your password on your local machine. Anyone who sits down at your computer will be able to access your personal information. If your browser asks you whether you want to save a password, say No!

iv) It is always a good idea to keep changing your passwords on a regular basis depending on the information you are trying to protect. Sensitive information = 3-6 months. Less sensitive but important information – 6 – 12 months.

3) **Surfing Internet and Online Transactions**

Most of the problems that may occur with the computer system generate while surfing Internet. Internet provides us with a lot of useful materials and tools to make the exchange of information swift and easier. It is a common place for hacking/phishing activity also where unaware users, who do not follow security guidelines, fall prey to.

i) One should never put your credit card info into a site you receive via e-mail. The address can be spoofed or redirected and you can give away your credit card without knowing it. Type in the address of the site you would like to visit yourself to ensure you are going to the correct place.

ii) Always check for a security icon on your browser. This is usually in the form of a "lock" icon to show that the site is appropriately secured. If you don't see this icon, don't put your credit card information in.

iii) Try to perform online transactions only on reputed portal, which has a security certificate for example www.indiatimes.com or Amazon.

iv) Save yourself from phishing attacks. Phishing is a scam where the perpetrator sends out legitimate-looking e-mails appearing to come from some of the popular sites like sbionline.com, incometaxindia.com. These sites generally claim that your IT refund has been processed and needs to be transferred to your bank account. The unsuspecting user might give in the bank details on the form provided. This info page does not belong to the legitimate site. If you fill out your personal information and submit it, the info will go to the "phisher" to be sold or used to steal your identity.

v) You should never save your password with the browser unless you are very sure that it is a dedicated personal machine like your laptop. Most web sites or browsers often ask you to save your password. This will make it so that anyone who has access to your browser has access to all of your personal information. And, if you become infected with certain viruses, your passwords will be published to the author of that virus.

vi) There are softwares called spywares that are downloaded automatically from many sites. Some spyware is disruptive – logs keystrokes to collect passwords etc, some used for ad purposes. Most of good anti-virus softwares have this inbuilt utility to identify and clean spywares from your machine.

vii) Always LOGOUT from the application once you are finished. If you don't log out of an application, especially a web based application, the next user may be able to hit back on the browser and access your personal information. Always LOG OUT and then close the browser when you have finished your session.

4) **Get information on secure websites and SSL certificates**

i) Try to make sure that the site where you wish to perform online transaction is using secure http. Just look for **https**:// in URL in place of simple **http://**.

ii) To make sure that the website you are browsing is safe and certified for online transactions, you must perform Secure Socket Layer (SSL) certificate verification.

iii) To perform SSL certificate verification, open the website and look for the lock symbol on the side of address bar of Internet Explorer or bottom status bar (for other browsers see help).

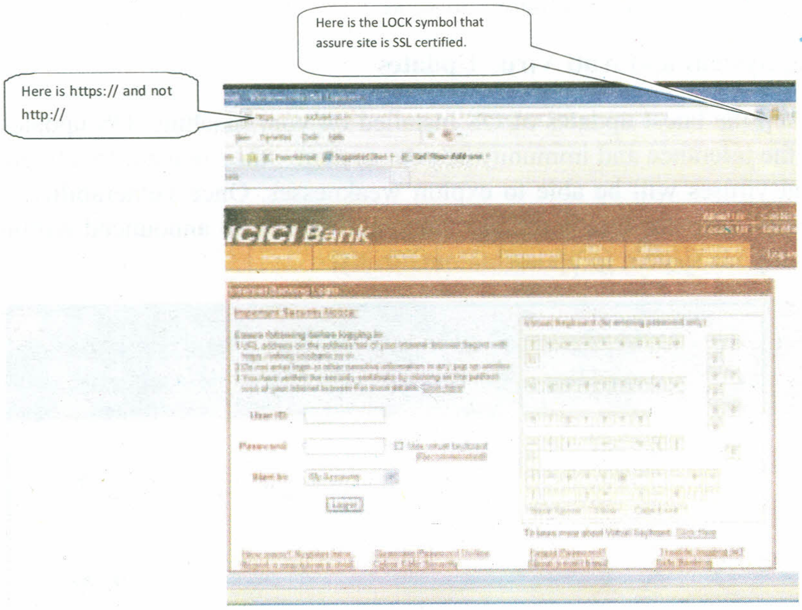


Fig. 3: SSL certified site

iv) Double click on the lock symbol and you will be able to see the certificate. It contains all the details such as name of the third party agency that has issues this, issuance date and expiry date of the certificate etc.

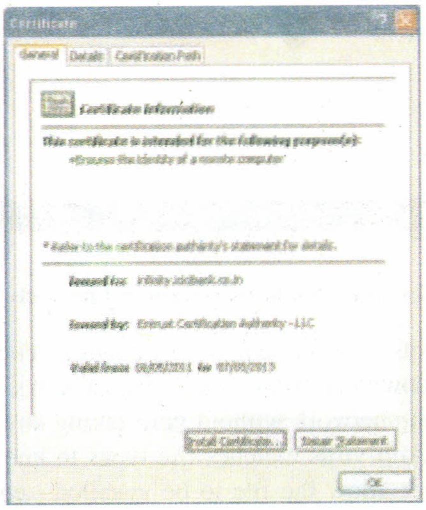


Fig. 4: SSL Certificate (see the validity till 2013)

5) **E-mail and Attachments**

   i) All the guidelines discussed under how to handle attachment problem in earlier topic i.e. Virus, worms and their handling should be applied in this case also.

   ii) All the e-mail users must use e-mail filters. E-mail filters like spam-filter etc. make sure that you do not receive unwanted e-mails in your Inbox.

   iii) Understand that E-mail is not secure. It is like sending a postcard written in pencil. As the card is delivered it makes numerous stops and can be altered or read by various people. Personal information should never be sent via e-mail – credit card, name phone address and date of birth in combination.

   iv) If you do not know the source, don't open the e-mail, simple delete it. Did you expect the e-mail? If not, send it back and ask for clarification. Addresses can be easily "spoofed" – change to seem like the mail was sent from someone else. A good rule is to be suspicious of every e-mail that you haven't asked someone to send.

6) **Operating System and Anti Virus Updates**

Always keep the latest updates of OS installed on your machine. OS updates improves the tolerance and immunity of your system – they make it less likely worms and viruses will be able to exploit weaknesses. Once vulnerability is announced, viruses for that particular vulnerability can be announced within days, so set your system to update automatically.

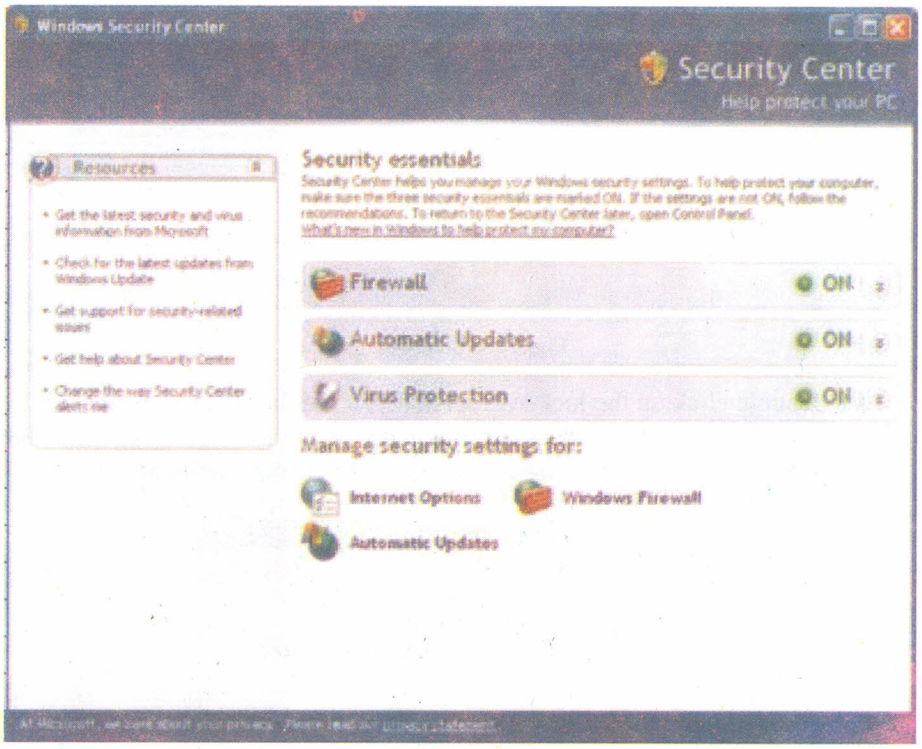


Fig. 5: Security Center that helps you control firewalls and security updates

Anti-virus protects your system from malicious code that is embedded in an attachment you download from e-mail, from a web site you visit or sent directly to you through the network without your taking any action besides turning on your computer. Anti-virus matches file types to known definitions for viruses and either doesn't allow the file to be installed, sends it to a quarantine area or deletes it.

Most OS and anti virus have their regular updates available online. It is highly recommended that the update should be set to automatic mode, in case your machine is connected to Internet. Otherwise, efforts should be made to obtain latest update and install it on the machine.

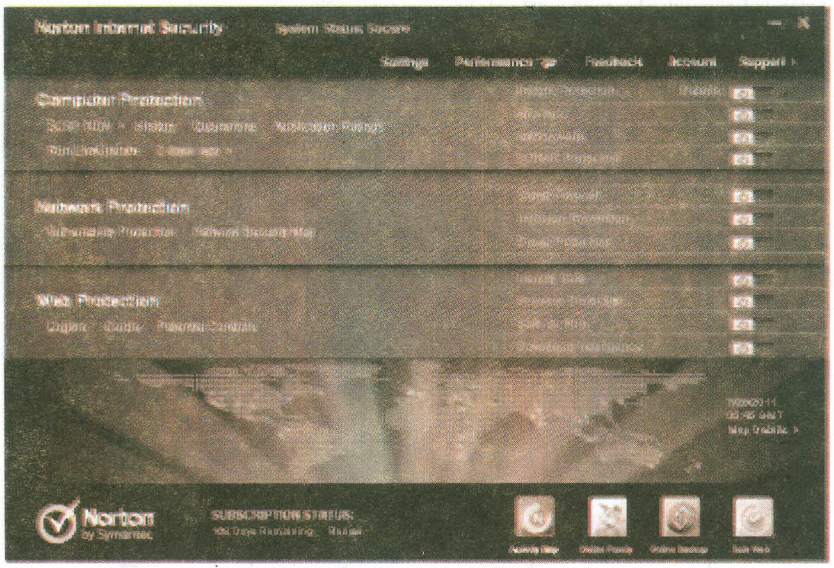


Fig. 6: The Screenshot of an Anti-virus software

7) **Firewall**

A personal firewall (sometimes called a desktop firewall) is a software application used to protect a single Internet-connected computer from intruders. Often compared to anti-virus applications, personal firewalls work in the background at the device level to protect the integrity of the system from malicious computer code by controlling Internet connections to and from a user's computer, filtering inbound and outbound traffic and alerting the user to attempted intrusions.

Windows XP has a built in firewall, all other OS's need a third party software application from one of the major vendors (such as McAfee, Norton).

To set it up on Windows XP:

http://www.microsoft.com/security/articles/use_icf.asp

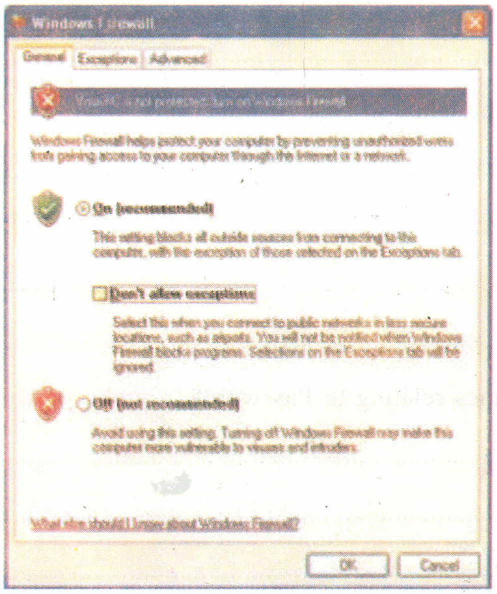


Fig. 7: Windows Firewall setting snapshot

8) Lock Screen Saver

Setting up a screen saver that locks when you step away from your desk is always a good idea. Set it to your own time limit and to require a password to activate. Lock your computer whenever you leave by hitting CTRL+ALT +DELETE and choosing "lock workstation"

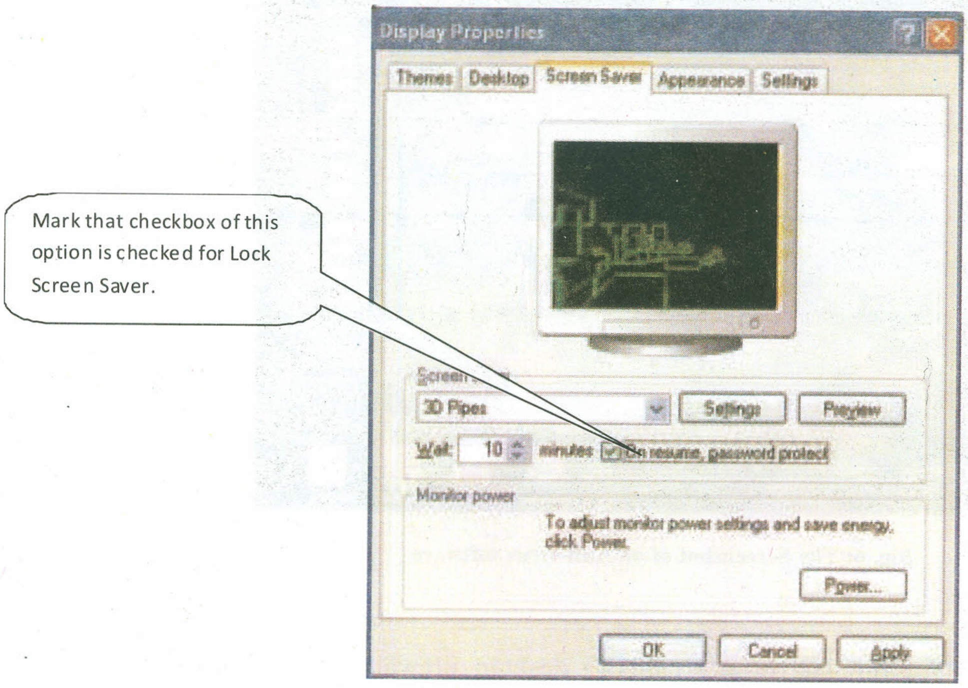


Fig. 8: Setting Lock Screen Saver

Check Your Progress 3

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) How to handle/avoid Viruses and Worms?

....

....

....

....

2) What action to be taken in case of infection?

....

....

....

....

3) Explain Guidelines relating to Passwords.

....

....

....

....

4) What is Firewall?

....

....

....

....

2.8 LET US SUM UP

This unit presents the need of Security Awareness from a point of view of both the end user as well as the organisation, be it the government or an enterprise.

The unit starts with outlining the fundamentals of Security Awareness where the need and justification of having an awareness programme is presented.

We have also discussed the security awareness programme life cycle that includes awareness programme design, materials development, programme implementation and post implementation activities. We have also proposed three models for implementing the security awareness programme.

The security awareness programme can be broken into two logical subprogrammes namely Awareness sessions and Awareness materials. Awareness Sessions are generally conducted in house to apprise users of policies and safeguards relating to security aspects. The materials help in reinforcing the concepts as well as maintaining the continuity which is most important. Since a new category of threats are discovered regularly, therefore the handling technique also needs to be updated and communicated to the users on a regular basis.

The best way to implement the security policies is to include them as a part of regular activities such as induction, follow-up, orientation programmes and signed agreements etc.

In the end, we have discussed basic security threats and guidelines on how to handle them. Guidelines relating to e-mails, choosing good passwords, setting firewalls, updates of OS and anti-virus etc. are discussed.

2.9 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) "Information security Awareness" is an activity simply to focus attention on security. Awareness programmes are intended to allow individuals to recognise IT security concerns and respond accordingly. At the same time, we have to remember that "Security Awareness" is not training and we have no intention to train people to handle the eventualities rather we are making them aware of when to raise alarm and to whom.

2) The four steps of life cycle of an Information security awareness programme:

   Steps 1 : Awareness Programme Design

   Step 2 : Awareness Material Development

   Step 3 : Awareness Programme Implementation

   Step 4 : Post-Implementation activities

3) **Partially Decentralised Model**

Training policy and strategy lie with a central authority, but implementation responsibilities are distributed. This model is for those organisations, which are multi-locations or multi-department. The training for department or location in charges can be conducted at a centralised place. The trained persons can then take care of imparting training for users under their control.

Fully Decentralised Model

Only policy development resides with a central authority and all other responsibilities are delegated to individual company components. This model is suitable for large organisation as it takes care of formulating a uniform policy for all the regional offices to follow.

Check Your Progress 2

1) An information security awareness programme process of a company consists of two major tasks:

- Awareness Sessions
- Awareness Materials

2) **Awareness Sessions**

In the awareness sessions, all employees should be taught the importance of information security. They should be told explicitly about the rules that must be followed and what to do if there is a violation. This activity acts as a pillar to Information Security Awareness campaign in any organisation.

Information security policy and standards are rendered ineffective if individuals at any level of the company are unaware of the importance of security policy, do not understand established standards or fail to perform required practices for any reason. Good security is "a state of mind" that can best be achieved by a programme or process that reinforces the concern for protecting our information assets and appropriate actions for doing so on a regular and ongoing basis.

3) The management may use any of the following tools to send their message across to their staff :

- E-mail messages
- Articles in the company's newsletter
- Magazines, internet articles for circulation
- Bulletins and alerts
- Posters
- Web announcements
- Quiz (to measure results of the programme)
- Giveaways – buttons, pens, certificates, t-shirt's, mouse pads, pen holders, coffee cups.

4) **Continuous awareness refresher courses**

All employees (employees, consultants, contractors, temporaries etc.) must receive some level of information security awareness and training. This training requirement must be included in all contracts. Workers must be provided with sufficient training and supporting reference materials to allow them to properly protect the company's information assets. Management should allocate sufficient on-the-job time for employees to acquaint themselves with the company's security rules, procedures and related ways of doing business.

Check Your Progress 3

1) To handle/avoid Viruses and Worms, we can take following steps:

   i) A user should make sure that the system has a good anti-virus programme installed on it. If the anti-virus is not available, the demand for the same must be raised immediately.

   ii) While sending/receiving e-mails, attachments should be avoided. The content of the file should be sent as a body of the e-mail rather than as an attachment.

   iii) Don't click links in e-mail unless you are absolutely sure you know the sender and recognise the URL.

   iv) Do not open/download an attachment/file unless you trust the source.

      a) Do you know the person who is sending you this file? E-mail addresses can be "spoofed" – the "from" address can be faked.

      b) Does it make sense that they are sending it to you?

      c) Microsoft NEVER sends operating system patches as e-mail attachments. They will ask you to visit the Microsoft Web site to download any software.

      d) If you're not sure, ask the sender to resend the attachment to verify that they actually sent it to you.

      e) Do not enter personal information into any web site form unless you are certain:

         - That the web site is authentic – clicking on a link in an e-mail can send you to any web site, make sure you are in the right place.

         - That the web site is secure – the lock icon in the bottom right corner of your browser will display as closed and highlighted.

2) Action to be taken in case of infection are the following:

   - Contact the Helpdesk of your organisation.

   - Remove your machine from the network to stop the spread of infection.

   - Wait for help to arrive.

3) Guidelines relating to Passwords are the following:

   - A password should be generally consisting of 8 characters or more, not a word, mixed case, mixed characters. Do not use your name or the name of a family member, your pets name, your favorite past time or sports team. These are easily guessed!

   - You should never share your password for the reason that the onus of any activity, legal or illegal, performed by using your password lies with you.

   - You should never save your password on your local machine. Anyone who sits down at your computer will be able to access your personal information. If your browser asks you whether you want to save a password, say No!

- It is always a good idea to keep changing your passwords on a regular basis depending on the information you are trying to protect. Sensitive information = 3-6 months. Less sensitive but important information – 6 – 12 months.

4) **Firewall**

A personal firewall (sometimes called a desktop firewall) is a software application used to protect a single Internet-connected computer from intruders. Often compared to anti-virus applications, personal firewalls work in the background at the device level to protect the integrity of the system from malicious computer code by controlling Internet connections to and from a user's computer, filtering inbound and outbound traffic and alerting the user to attempted intrusions.

2.10 SUGGESTED READINGS

- Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole, Sunit Belapure, Wiley.
- Information Security: Principles and Practices by Mark Merkow, James Breithaupt, Pearson Education.
- Mark B. Desman, Building an Information Security Awareness Program, Auer Bach Publications.
- Principles of Computer Security by Wm. Arthur Conklin, McGraw Hill.
- Principles of Information Security by Michael Whitmankennesaw, Course Technology.
- www.isea.gov.in.

UNIT 3 INFORMATION SECURITY: OVERVIEW

Structure

3.0 INTRODUCTION

Information security is a matter of great concern. To protect information different techniques are used by the organizations. Especially when the information is used on the internet and it moves in the cyber world from one compute to another computer crossing different geographical boundaries. There are chances of information theft on the way by some malicious users. To protect information against such threats the data protection is a must. Here in this unit some techniques are discussed to provide the overview of how we can safeguard vital information against such threats.

3.1 OBJECTIVES

After studying this unit, you should be able to understand:

- Information security and principle;
- need of Information security;
- security model iPhone security issues;
- security model and architecture; and
- risk management.

3.2 INFORMATION SECURITY

Information security deals with the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction The terms information security, computer security and information assurance are used in each other's place. The fields mentioned above are interrelated to each other and have common objective of protecting the confidentiality, integrity and availability of information; however, some differences exists between them. The differences among them are based on the approach to the subject, the methodologies used and the areas of concentration. Information security takes care of confidentiality, integrity and availability of data regardless of the type of data like: electronic, print or other forms. The main focus of Computer security is ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

Governments, military, corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Majority of the information is now gathered, processed and stored on electronic computers and moved to other computers across the networks. Now if the confidential information about a business' customers or finances or new product line leak out into the hands of a competitor, such a breach of security could lead to a great loss in business, law suits or even bankruptcy of the business. Keeping this information private is a business requirement and also in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures Information security has evolved significantly in recent years. There are multiple ways of getting entry into the field as a career. It consists of many areas for specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science etc.

History

Since the early days of writing, heads of state and military commanders analysed that it was important to provide some mechanism to protect the privacy of written correspondence and to have some way to detect tampering.

Julius Caesar is credited with the invention of the Caesar cipher ca. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands.

World War II brought about many advancements in information security and marked the beginning of the professional field of information security.

The end of the 20^{th} century and early years of the 21^{st} century saw rapid advancements in telecommunications, computing hardware and software and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through a network generically called the Internet or World Wide Web.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations – all sharing the common goals of ensuring the security and reliability of information systems.

3.3 BASIC PRINCIPLES

Key concepts

The core principles of information security for over twenty years are confidentiality, integrity and availability. There is never ending debate about extending this classic trio. Other principles such as Accountability have also been proposed for addition – it has been pointed out that issues such as Non-Repudiation do not fit well within the three core concepts and as regulation of computer systems has increased, legality is becoming a key consideration for practical security installations.

The six atomic elements of information was an alternative model for classic CIA proposed by, Donn Parker in 2002. The elements are confidentiality, possession, integrity, authenticity, availability and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

Confidentiality

Confidentiality refers to protection of the exposure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Breaking of confidentiality may have different forms. As an example if we allow someone to look over our shoulder at our computer screen while we have private data displayed on it could be a breaking of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breaking of confidentiality. If someone is narrating private information on the telephone that is again a breach of confidentiality if the caller is an unauthorized body.

Confidentiality is mandatory for maintaining the privacy of the people whose personal information a system holds.

Integrity

In information security, integrity means that data should remain as it was it should not be modified. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID model of transaction processing. Integrity is not met when a message is actively changed in transit. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

Any information system is successful if it serves the purpose it is intended to do, in this case the information must be available when it is needed. Computing systems are used to store and process the information, the security controls used to protect it and the communication channels used to access it must be functioning correctly. The aim of high availability systems is to remain available at all times, preventing service disruptions due to power outages, hardware failures and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It states that one party of a transaction cannot refuse having received a transaction nor can the other party refuse having sent a transaction.

Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation.

3.4 NEED OF INFORMATION SECURITY

Lifeblood of all organizations is information and it can exist in multiple forms. It can be printed or written on paper, stored electronically, transmitted by mail or by electronic means, shown in films or spoken in conversation. If we talk about todays world , in this competitive business environment, such information is constantly under threat from many sources. The sorces can be internal, external, accidental or malicious. With the advent of new new technologies to store, transmit and retrieve information, we have all invited increased numbers and types of threats.

Acknowledging all the above mention points we feel that there is a need to establish a comprehensive Information Security Policy within all organizations. In order to ensure the confidentiality, integrity and availability of both vital corporate information and customer information. The standard for Information Security Management System (ISMS) ISO/ IEC 27001:2005 has fast become one of the world's established biggest sellers.

3.5 ABOUT SECURITY MODEL

Computer and information security forms major portion in any enterprise. Each area has security vulnerabilities and, hopefully, some corresponding solutions that provide the security level a better protection. Not understanding the different areas and security levels of network devices, operating systems, hardware, protocols and applications can cause security vulnerabilities that can affect the environment as a whole.

There are two fundamental concepts in computer and information security are the security model, which designs how security is to be implemented-in other words, providing a "blueprint"– and the architecture of a computer system, which fulfills this blueprint.

A security policy guides that how data is accessed, required level of security and what actions should be taken if in case these requirements are not met. The policy outlines the expectations of a computer system or device. A *security model* is a statement that outlines the requirements necessary to properly support and implement a certain security policy. If a security policy dictates that all users must be identified, authenticated and authorized before accessing network resources, the security model might lay out an access control matrix that should be constructed so that it fulfills the requirements of the security policy. If a security policy states that no one from a lower security level should be able to view or modify information at a higher security level, the supporting security model will outline the necessary logic and rules that need to be implemented to ensure that under no circumstances can a lower-level subject access a higher-level object in an unauthorized manner. A security model provides a deeper explanation of how a computer operating system should be developed to properly support a specific security policy.

3.6 PATH TO EFFECTIVE INFORMATION SECURITY MANAGEMENT

Following are the key steps that every company implementing an Information Security Management System should consider:

- **Purchase the Standard**

  Before you can begin preparing for your application, you will require a copy of the standard. You should read this and make yourself familiar with it.

- **Review free Guidance Documents, Publications and Software**

  There are a wide range of free guidance documents, quality publications and software tools designed to help you understand, implement and become registered to an Information Security Management System.

- **Consider Training**

  One can take help of training courses available that help how to implement and assess your Information Security Management System.

- **Assemble a Team and Agree Your Strategy**

  Before starting we should begin the entire implementation process by preparing our organizational strategy with top management. At this point of time we should determine the Scope of your Registration – whether the system will be adopted company wide or by one or more departments.

- **Review Consultancy Options**

  we can discuss this matter with independent consultanat and receive advice on how to implement information security management system.

- **Undertake a Risk Assessment**

  During this phase we should study and review all potential security ruptures. This should not relate solely to IT systems, but should encompass all sensitive information within your organization.

- **Develop a Policy Document**

  This will demonstrate management support and commitment to the Information Security Management System process.

- **Develop Supporting Literature**

  Put together a Statement of Applicability and Procedures to support your security policy. This will cover a range of areas including asset clarification and control, personal security, physical and environmental security and business continuity management.

- **Choose a Certification Body**

  The certification body is a third party, such as BSI Management Systems, who come and assess the effectiveness of our Information Security Management System against the industry best practice standard, ISO/IEC 27001:2005. BSI issues a certificate if the ISMS meets the requirements of the standard. Choosing a certification body can be a complex issue as there are so many operating in the market. Factors to consider include industry and auditing experience, geographic coverage and service level offered. The key is to find the certification body who can best meet your requirements. A great place to start is by contacting BSI Management Systems.

- **Implement Your Information Security Management System**

  The key to implementation is communication and training. During the implementation phase everyone begins operating to the procedures of the management system.

- **Gain Registration/Certification**

  We should arrange our previous assessment with our registrar. At this stage the registrar will study our Information Security Management System and determine whether you should be recommended for registration or not.

- **Continual Assessment**

  Once we have received registration and have been awarded our certificate,we can start to advertise our success and promote our business. Our ISMS will be checked from time to time by our registrar to make sure that it continues to meet the requirements of the standard.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Write a note on information security.

....

....

....

....

2) What do you understand by non-repudiation?

....

....

....

....

3) Discuss the need of information security.

....

....

....

....

4) Write a note on security model.

....

....

....

....

3.7 IPHONE APPLICATION DEVELOPMENT SECURITY ISSUES

Since Apple released the iPhone in 2007, it ruling in the mobile phones market. In fact, Canalys forecasts Apple capturing 21.3% of the mobile market in 2010. The iPhone came across very less significant platform security issues along the way. There has been a continual effort on jail breaking the iPhone and unlocking it. security news related to the iPhone pays more attention on the platform itself, while less attention has been paid to individual applications in the app store. What are the most common security risks affecting iPhone applications? Based on our experience testing iPhone applications, we have compiled a top 5 list of security issues for developers:

- **Sensitive data unprotected at rest**

  Mobile applications rely a lot on the software functionality to provide its users with what they absolutely need when they are on the move. Many applications, involve representing or even storing, sensitive data. Many iPhone applications read and display sensitive data, such as medical lab test results or personal and business oriented financial data. For example, the Care 360 Mobile iPhone application allows doctors and medical professionals to retrieve and view lab results from Quest Diagnostics. Many large banks also provide mobile applications to provide better user experience than the Safari web browser for online banking. The work of such applications involves handling sensitive data, most users will ever possess. Additionally, many applications also provide a variety of "remember me" functionality. Protecting this data from malicious adversary is important for both the user and the application provider. The solution to this problem is careful architecture design with a risk-based approach to help decide the security posture the application has towards data storage. Once we very well know the risk, it is very important to protect sensitive data that must reside on the device using a combination of strong cryptography and the Apple Keychain services or equivalent cryptographic constructs, to protect this sensitive data while at rest.

- **Buffer overflows and other C programming issues**

  The iPhone development platform is based on Objective-C. Objective-C provides a much cleaner environment for the programmer when compared to C. It helps in preventing many common C programming errors, which can result in exploitable bugs and flaws in an application. If a developer writes an application purely from within the confines of Objective-C using the Foundation, UIKit and other pure Objective-C frameworks, the application is relatively safe from most of the security issues that afflict C programs. For example, the NSString class prevents buffer overflow bugs effectively in most cases (assuming there are no flaws in the underlying NSString implementation). Another advantage of Objective-C environment of the iPhone is that all object allocations go on the heap, which helps prevent stack overflows since directly programmer controlled memory does not live on the stack. The developer has to take care of allocation and deallocation of objects, but the complexity is largely hidden from the developer compared to a C implementation.

  However, some parts of the iPhone SDK require the developer to return to the standard C. This is an all bets are off proposition that eliminates the safety provided by the Objective-C platform. It is common to build and include C libraries in an iPhone application to avoid re-implementing code. This means going from relatively safe Objective-C libraries and moving to less safe C style strings for libraries like SQLite, a core part of many iPhone applications and Buffer overflows are one of the various issues that plague C programs.

Vulnerabilities can stem from heap overflows, format string attacks, integer overflows and other more subtle issues that are relevant when developing in C for iPhone.

Generally avoiding C libraries when at all possible is ideal. However, when C and C libraries are required developers must follow best practices derived over the lifetime of the C programming language. When observing best practices mistakes may still occur. Development teams must use safe string libraries and individual developers must understand the risks and vulnerabilities that can occur when writing code in C.

- **Secure communications to servers**

  Every useful application that processes sensitive user data will connect back to some server component. Developers have to face the challenge of having to protect sensitive data in transmission as it traverses the Internet and sometimes even insecure wireless media. The data is protected using encryption; that must be implemented correctly.

  Effective encryption entails avoiding reinventing the wheel and using trusted libraries that have been thoroughly reviewed. The iPhone SDK is, largely, like any other SDK regarding its SSL libraries. Developers should be aware while using the URL loading library as the way differs from application to application. The default state of operation for the URL loading library is to fail on an invalid server certificate. However, during development it is often required to use an invalid certificate. Failure to use the libraries properly can result in weak client to server communications that allow a malicious adversary to compromise client to server communications.

- **Patching your application**

  The App Store could be your worst enemy, a proper risk assessment of an organization's tolerance for risk should be conducted to determine if the app store policy will match up with and be acceptable, for any given application. Apple maintains tight control over the App Store and it will not be possible to issue a release in a very short (24-48) hour period in most cases. The Apple approval process generally takes at least a week. If the application has any issues that would cause it to fail, the approval process of the new build could take weeks to reach customers.

  Unfortunately, the organization can help a bit regarding the risk associated with this issue. The best bet is to make sure that developers have a clear understanding of app store policy and that the testing process is thorough and proactively identifies issues that would cause the application to fail the approval process.

- **The platform itself**

  An important component of application security is user awareness. Users often look and treat their mobile, Internet connected, devices with a different level of care compared to a laptop or desktop. Password policies, anti-virus software and at least some awareness that their computer may contain sensitive data and that it requires protection is the norm for most users. Mobile devices are often lost, not password protected and get treated with a lower level of security awareness. This means that a user could easily lose their phone to a malicious individual and have their sensitive data compromised.

  Thus, it is necessary to attempt to make a mobile user aware of the risks they are exposed to through well constructed documentation and application design. A mobile user who is more security conscious may take efforts to secure their environment more, such as by using a PIN or pass phrase to secure their device and subscribing to Apple services that can help locate and disable lost or stolen devices. From a developers point of view the important that thing is to alert the user when they are making security sensitive actions via visual cues and or dialogs/text. Users will generally get attracted towards whatever is quickest and easiest for them.

3.8 APPLICATION DEVELOPMENT SECURITY

Application development security is a critical enterprise priority

Today applications are weak link in enterprise security. Hackers now use software vulnerabilities or malicious code and backdoors embedded in application code to gain access to companies private information. Application development security forms important part in protecting the enterprise. Organizations must employ solutions to scan code, seeking to find both malicious code as well as flaws in software that could create vulnerabilities. Application development security products have high cost and maintenance. And most are unable to scan an entire application, because the software today is often combination of code from a variety of sources-the source code is simply unavailable for study. That's why Veracode has developed an innovative new method for achieving application development security-the industry's only automated, on-demand, application security testing solution.

Veracode delivers cost-effective, on-demand, application development security

Veracode was founded by security experts from @stake, Guardent, Verisign and Symantec to provide a more effective and cost-efficient way to ensure application development security-and Veracode SecurityReview® delivers on both counts. SecurityReview is built on the software-as-a-service model, delivering code analysis as an on-demand service. That means organizations can avoid capital investment in software security assurance products, thus allowing companies to easily scale secure software development testing. And SecurityReview uses multiple testing techniques to offer the most comprehensive secure software testing solution in the industry today. In addition to dynamic analysis (for web services security) and manual penetration testing, Veracode uses static binary analysis to scan binary (compiled or "byte" code) instead of source code, allowing SecurityReview to provide 100 percent coverage of any application. No other testing solution provides coverage this complete.

Enhance security and speed development with automated application testing

Veracode SecurityReview enables organizations to speed secure software development while improving security at the same time. SecurityReview uses a milestone-based approach to testing that embeds secure coding best-practices in the software development life cycle. The result is reduced costs, more secure software and shorter development cycles. Because Veracode is a truly outsourced service, developers can be freed to focus on building secure applications and meet project deadlines instead of learning and maintaining testing products. And with testing results prioritized by risk level and ease of remediation-and delivered in an online environment-globally distributed teams of developers can collaborate to fix flaws quickly and cost-effectively.

3.9 SECURITY MODEL AND ARCHITECURE

Computer and information security consists of many areas within an organization. Each area is susceptible to security vulnerabilities and, hopefully, some corresponding solutions that raise the security level and provide better protection. Not taking into account the different areas and security levels of network devices, operating systems, hardware, protocols and applications can cause security vulnerabilities that can affect the environment as a whole.

Two fundamental concepts in computer and information security are the security model, which outlines how security is to be implemented – in other words, providing a "blueprint" – and the architecture of a computer system, which fulfills this blueprint.

A security policy guides how data is accessed, what level of security is required and what actions should be taken when these requirements are not met. The policy shows the expectations of a computer system or device. A security model is a statement that outlines the requirements

Check Your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Write a note on secure communications to server.

....

....

....

....

2) Write a note on buffer overflows and other C programming issues.

....

....

....

....

3) Justify the statement: application development security is a critical enterprise priority.

....

....

....

....

4) Write a note on security model and architecture.

....

....

....

....

3.10 ENTERPRISE INFORMATION SECURITY ARCHITECTURE (EISA)

Enterprise information security architecture (EISA) is the study of implementing a comprehensive and rigorous method for describing a current and/or future structure

and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. Although often associated strictly with information security technology, it relates more broadly to the security practice of business optimization in that it addresses business security architecture, performance management and security process architecture as well.
Within the financial institutions around the world Enterprise information security architecture is becoming a common practice. In order to align business strategy and IT security information security architecture is used. As such, enterprise information security architecture allows traceability from the business strategy down to the underlying technology.

Positioning

Gartner in their whitepaper called "Incorporating Security into the Enterprise Architecture Process" first formally positioned Enterprise information security. This was published on 24 January 2006. After this publication, security architecture has transformed from being a silo based architecture to an enterprise focused solution that incorporates business, information and technology. The picture below shows a one-dimensional view of enterprise architecture as a service-oriented architecture. It represents that security is added to enterprise architecture family. Business architecture, information architecture and technology architecture use to be called BIT for short. Now with security as part of the architecture family it has become BITS.

Security architectural change imperatives now include things like

- Business roadmaps
- Legislative and legal requirements
- Technology roadmaps
- Best practices
- Industry trends
- Visionaries

Goals

- Provide structure, coherence and cohesiveness.
- Must enable business-to-security alignment.
- Defined top-down beginning with business strategy.
- Ensure that all models and implementations can be traced back to the business strategy, specific business requirements and key principles.
- Provide abstraction so that complicating factors, such as geography and technology religion, can be removed and reinstated at different levels of detail only when required.
- Establish a common "language" for information security within the organization

Methodology

The study of enterprise information security architecture involves creating an architecture security framework to describe a series of "current", "intermediate" and "target" reference architectures and applying them to align programs of change. These frameworks describe in detail the roles organizations should have, entities and relationships that exist or should exist to perform a set of business processes.

The aim of framework is to provide a rigorous technique of classification and the study of nature and existence that clearly identifies what processes a business performs and detailed information about how those processes are executed and secured. The result is a set of an object that describe in varying degrees of detail exactly what and how a business operates and what security controls are required. The objects are often graphical.

The levels of detail will change according to affordability and other practical considerations, decision makers are well equipped with the means to make informed decisions about where to invest resources, where to realign organizational goals and processes and what policies and procedures will support core missions or business functions.

A strong enterprise information security architecture process helps to answer basic questions like:

- Is the current architecture supporting and adding value to the security of the organization?
- How might a security architecture be modified so that it adds more value to the organization?
- Based on what we know about what the organization wants to accomplish in the future, will the current security architecture support or hinder that?

Enterprise information security architecture implementation consists of documenting the organization's strategy and other necessary details such as where and how it operates. The next step is documenting discrete core competencies, business processes and how the organization interacts with itself and with external parties such as customers, suppliers and government entities.

Having documented the organization's strategy and structure, the architecture process then flows down into the discrete information technology components such as:

- Organization charts, activities and process flows of how the IT Organization operates
- Organization cycles, periods and timing
- Suppliers of technology hardware, software and services
- Applications and software inventories and diagrams
- Interfaces between applications – that is: events, messages and data flows
- Intranet, Extranet, Internet, e-commerce, EDI links with parties within and outside of the organization
- Data classifications, Databases and supporting data models
- Hardware, platforms, hosting: servers, network components and security devices and where they are kept
- Local and wide area networks, Internet connectivity diagrams

It should be noted that whenever possible all the above mentioned points should relate explicitly to the organization's strategy, goals and operations. The enterprise information security architecture should document the current state of the technical security components listed above, as well as an ideal-world desired future state and finally a "Target" future state which is the result of engineering tradeoffs and compromises vs. the ideal. Mostly the outcome is a nested and interrelated set of models, usually managed and maintained with specialised software available on the market.

Such exhaustive mapping of IT dependencies has notable overlaps with both metadata in the general IT sense and with the ITIL concept of the Configuration

Management Database. Maintaining the accuracy of such data can be a significant challenge.

In addition to the models and diagrams a set of best practices which are objected at securing adaptability, scalability, manageability etc. These systems engineering best practices are not unique to enterprise information security architecture but they are considered important to the success nonetheless. They involve such things as componentization, asynchronous communication between major components, standardization of key identifiers and so on.

Appropriate positioning of information security architecture is required in an organization. This is analogous to city-planning.

An intermediate outcome of an architecture process is a comprehensive inventory of business security strategy, business security processes, organizational charts, technical security inventories, system and interface diagrams and network topologies and the explicit relationships between them. The inventories and diagrams are merely tools that support decision making. But this is not sufficient. It must be a living process.

The organization must design and implement a process that ensures continual movement from the current state to the future state. The future state will generally be a combination of one or more

- Closing gaps that are present between the current organization strategy and the ability of the IT security dimensions to support it
- Closing gaps that are present between the desired future organization strategy and the ability of the security dimensions to support it
- Necessary upgrades and replacements that must be made to the IT security architecture based on supplier viability, age and performance of hardware and software, capacity issues, known or anticipated regulatory requirements and other issues not driven explicitly by the organization's functional management.
- On a regular basis, the current state and future state are redefined to account for evolution of the architecture, changes in organizational strategy and purely external factors such as changes in technology and customer/vendor/ government requirements.

High-level security architecture framework

Enterprise information security architecture frameworks is a subpart of enterprise architecture frameworks. If one had to reduce the complexity of the conceptual abstraction of enterprise information security architecture within a generic framework, the picture on the right would be acceptable as a high-level conceptual security architecture framework.

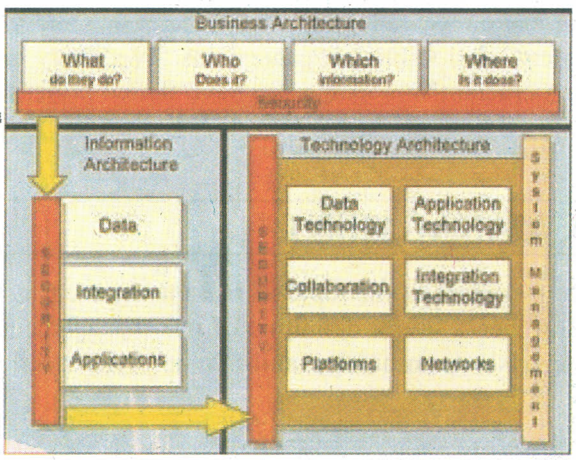


Fig. 1

Other open enterprise architecture frameworks are:

- The U.S. Department of Defense (DoD) Architecture Framework (DoDAF),
- Extended Enterprise Architecture Framework (E2AF) from the Institute For Enterprise Architecture Developments.
- Federal Enterprise Architecture of the United States Government (FEA)
- Capgemini's Integrated Architecture Framework
- The UK Ministry of Defence (MOD) Architecture Framework (MODAF)
- NIH Enterprise Architecture Framework
- Open Security Architecture
- Information Assurance Enterprise Architectural Framework (IAEAF)
- SABSA framework and methodology
- Service-Oriented Modeling Framework (SOMF)
- The Open Group Architecture Framework (TOGAF)
- Zachman Framework

Relationship to other IT disciplines

Enterprise information security architecture forms very important part of the information security technology governance process at any organization of significant size. Most of the companies are making use of a formal enterprise security architecture process to support the governance and management of IT.

However, as stated in the starting of this article principly it relates more broadly to the practice of business optimization in that it addresses business security architecture, performance management and process security architecture as well. Enterprise Information Security Architecture also deals with IT security portfolio management and metadata in the enterprise IT sense.

Information security professionalism

Information security professionalism represents a collection of knowledge that is required in the people working in Information security and similar fields, which should have been eventually demonstrated through certifications from well respected organizations.

It consists of the education process which is needed to perform different tasks in these fields.

The usage of Information technology is always increasing and is spreading to vital infrastructure for civil and military organizations. Everybody can get involved in the Cyberwar. It is crucial that a nation can have skilled professional to defend its vital interests.

3.11 RISK MANAGMENT

A comprehensive treatment of the topic of risk management is beyond the scope of this article. However, a useful definition of risk management will be provided as well as some basic terminology and a commonly used process for risk management.

The CISA Review Manual 2006 provides the following definition of risk management: "Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."

Two points in this definition that may need some further clarification. First, the process of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerability emerge every day. Second, the choice of countermeasure (computer)s (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure and the value of the informational asset being protected.

Risk may be defined as the likelihood that something bad will happen that may cause harm to an informational asset or loss of the asset. A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat may be defined as anything that has the potential or capability to cause harm.

The possibility that a threat is vulnerable to cause harm which creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. If we consider the case of information security, the result is a loss of availability, integrity and confidentiality and possibly other losses. It should be pointed out that it is not possible to identify all risks, nor is it possible to eradicate all risk. The remaining risk is called residual risk.

A risk assessment is done with the help of team of people who have knowledge of specific areas of the business. Membership of the team may be different over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

According to the research the most susceptible point in most information systems is the human user, operator, designer or other human The ISO/IEC 27002:2005 Code of practice for information security management recommends the following be examined during a risk assessment:

- security policy,
- organization of information security,
- asset management,
- human resources security,
- physical and environmental security,
- communications and operations management,
- access control,
- information systems acquisition, development and maintenance,
- information security incident management,
- business continuity management and
- regulatory compliance.

In broad terms, the risk management process consists of:

1) Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.

2) Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.

3) Conduct a vulnerability assessment and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.

4) Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.

5) Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness and value of the asset.

6) Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

Considering any given risk, Executive Management can agree to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. By using out sourcing to another business ,in some cases, the risk can be transferred. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk. This is itself a potential risk.

Controls

When Management makes decision to reduce the risk, it may do so by making use of one of the three different types of control.

Administrative

Administrative controls are also called procedural controls which includes approved written policies, procedures, standards and guidelines.The framework for running the business and managing people is formed with the help of administrative controls. They provide people with the knowledge on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed - the Payment Card Industry (PCI) Data Security Standard required by Visa and Master Card is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

Logical

Logical controls are also called technical controls make use of software and data to observe and control access to information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists and data encryption are logical controls.

An important logical control that is frequently overlooked is the principle of least privilege. The principle of least privilege needs that an individual, programme or system process should not be granted any more access rights apart from which are

3.12 LET US SUM UP

Information security is the ongoing process of exercising due care and due diligence to protect information and information systems, from unauthorized access, use, disclosure, destruction, modification or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring and detection, incident response and repair, documentation and review. This makes information security an indispensable part of all the business operations across different domains.

3.13 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Information security deals with the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction The terms information security, computer security and information assurance are used in each other's place. The fields mentioned above are interrelated to each other and have common objective of protecting the confidentiality, integrity and availability of information; however, some differences exists between them. The differences among them are based on the approach to the subject, the methodologies used and the areas of concentration. Information security takes care of confidentiality, integrity and availability of data regardless of the type of data like: electronic, print or other forms. The main focus of Computer security is ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

   Governments, military, corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Majority of the information is now gathered , processed and stored on electronic computers and moved to other computers across the networks. Now if the confidential information about a business' customers or finances or new product line leak out into the hands of a competitor, such a breach of security could lead to a great loss in business, law suits or even bankruptcy of the business. Keeping this information private is a business requirement and also in many cases also an ethical and legal requirement.

2) In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It states that one party of a transaction cannot refuse having received a transaction nor can the other party refuse having sent a transaction.

   Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation.

3) Lifeblood of all organizations is information and it can exist in multiple forms. It can be printed or written on paper, stored electronically, transmitted by mail or by electronic means, shown in films or spoken in conversation. If we talk about todays world , in this competitive business environment, such information is constantly under threat from many sources. The sorces can be internal, external, accidental or malicious. With the advent of new new technologies to store, transmit and retrieve information, we have all invited increased numbers and types of threats. Acknowledging all the above mention points we feel that there is a need to establish a comprehensive Information Security Policy within all organizations. In order to ensure the confidentiality, integrity and availability of both vital corporate information and customer information. The standard

for Information Security Management System (ISMS) ISO/IEC 27001:2005 has fast become one of the world's established biggest sellers.

4) Computer and information security forms major portion in any enterprise. Each area has security vulnerabilities and, hopefully, some corresponding solutions that provide the security level a better protection. Not understanding the different areas and security levels of network devices, operating systems, hardware, protocols and applications can cause security vulnerabilities that can affect the environment as a whole.

   There are two fundamental concepts in computer and information security are the security model, which designs how security is to be implemented-in other words, providing a "blueprint" – and the architecture of a computer system, which fulfills this blueprint.A security policy guides that how data is accessed, required level of security and what actions should be taken if in case these requirements are not met. The policy outlines the expectations of a computer system or device. A *security model* is a statement that out- lines the requirements necessary to properly support and implement a certain security policy. If a security policy dictates that all users must be identified, authenticated and au- thorized before accessing network resources, the security model might lay out an access control matrix that should be constructed so that it fulfills the requirements of the security policy. If a security policy states that no one from a lower security level should be able to view or modify information at a higher security level, the supporting security model will outline the necessary logic and rules that need to be implemented to ensure that under no circumstances can a lower-level subject access a higher-level object in an unauthorized manner. A security model provides a deeper explanation of how a computer operating system should be developed to properly support a specific security policy.

Check Your Progress 2

1) Every useful application that processes sensitive user data will connect back to some server component. Developers have to face the challenge of having to protect sensitive data in transmission as it traverses the Internet and sometimes even insecure wireless media. The data is protected using encryption; that must be implemented correctly.

   Effective encryption entails avoiding reinventing the wheel and using trusted libraries that have been thoroughly reviewed. The iPhone SDK is, largely, like any other SDK regarding its SSL libraries. Developers should be aware while using the URL loading library as the way differs from application to application. The default state of operation for the URL loading library is to fail on an invalid server certificate. However, during development it is often required to use an invalid certificate. Failure to use the libraries properly can result in weak client to server communications that allow a malicious adversary to compromise client to server communications.

2) The iPhone development platform is based on Objective-C. Objective-C provides a much cleaner environment for the programmer when compared to C. It helps in preventing many common C programming errors, which can result in exploitable bugs and flaws in an application. If a developer writes an application purely from within the confines of Objective-C using the Foundation, UIKit and other pure Objective-C frameworks, the application is relatively safe from most of the security issues that afflict C programmes. For example, the NSString class prevents buffer overflow bugs effectively in most cases (assuming there are no flaws in the underlying NSString implementation). Another advantage of Objective-C environment of the iPhone is that all object allocations go on the heap, which helps prevent stack overflows since directly

programmer controlled memory does not live on the stack. The developer has to take care of allocation and deallocation of objects, but the complexity is largely hidden from the developer compared to a C implementation.

However, some parts of the iPhone SDK require the developer to return to the standard C. This is an all bets are off proposition that eliminates the safety provided by the Objective-C platform. It is common to build and include C libraries in an iPhone application to avoid re-implementing code. This means going from relatively safe Objective-C libraries and moving to less safe C style strings for libraries like SQLite, a core part of many iPhone applications and Buffer overflows are one of the various issues that plague C programmes. Vulnerabilities can stem from heap overflows, format string attacks, integer overflows and other more subtle issues that are relevant when developing in C for iPhone.

Generally avoiding C libraries when at all possible is ideal. However, when C and C libraries are required developers must follow best practices derived over the lifetime of the C programming language. When observing best practices mistakes may still occur. Development teams must use safe string libraries and individual developers must understand the risks and vulnerabilities that can occur when writing code in C.

3) Today applications are weak link in enterprise security. Hackers now use software vulnerabilities or malicious code and backdoors embedded in application code to gain access to companies private information. Application development security forms important part in protecting the enterprise. Organizations must employ solutions to scan code, seeking to find both malicious code as well as flaws in software that could create vulnerabilities. Application development security products have high cost and maintenance. And most are unable to scan an entire application, because the software today is often combination of code from a variety of sources-the source code is simply unavailable for study. That's why Veracode has developed an innovative new method for achieving application development security-the industry's only automated, on-demand, application security testing solution.

4) Computer and information security consists of many areas within an organization. Each area is susceptible to security vulnerabilities and, hopefully, some corresponding solutions that raise the security level and provide better protection. Not taking into account the different areas and security levels of network devices, operating systems, hardware, protocols and applications can cause security vulnerabilities that can affect the environment as a whole.

Two fundamental concepts in computer and information security are the security model, which outlines how security is to be implemented – in other words, providing a "blueprint" – and the architecture of a computer system, which fulfills this blueprint.A security policy guides how data is accessed, what level of security is required and what actions should be taken when these requirements are not met. The policy shows the expectations of a computer system or device. A security model is a statement that outlines the requirements.

Check Your Progress 3

1) Enterprise information security architecture (EISA) is the study of implementing a comprehensive and rigorous method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's core goals and strategic direction. Although often associated strictly with information security technology, it relates more

broadly to the security practice of business optimization in that it addresses business security architecture, performance management and security process architecture as well.

Within the financial institutions around the world Enterprise information security architecture is becoming a common practice. In order to align business strategy and IT security information security architecture is used. As such, enterprise information security architecture allows traceability from the business strategy down to the underlying technology.

2) Information security professionalism represents a collection of knowledge that is required in the people working in Information security and similar fields, which should have been eventually demonstrated through certifications from well respected organizations.

   It consists of the education process which is needed to perform different tasks in these fields. The usage of Information technology is always increasing and is spreading to vital infrastructure for civil and military organizations. Everybody can get involved in the Cyberwar. It is crucial that a nation can have skilled professional to defend its vital interests.

3) Information security must be able to prevent the information from unauthorized access throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected in both states while in motion and while at rest. Throughout its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems. There are multiple ways the information and information systems can be threatened. If we want to protect the information completely during its lifetime, each component of the information processing system must have its own protection mechanisms. Defense in depth is way of building up, layering on and overlapping of security measures. The strength of any system is no greater than its weakest link. Using a defence in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

   Recall the earlier discussion about administrative controls, logical controls and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in-depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion and network security, host-based security and application security forming the outermost layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

4) Cryptography is used by information security to convert usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been converted or encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is a process used in information security to prevent the information from unauthorized or accidental disclosure while the information is being transmitted and while information is in storage.

   Cryptography in information security has other useful applications which include improved authentication methods, message digests, digital signatures, non-repudiation and encrypted network communications. Application which important to perform a task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read E-mail and surf the Web. Breaching of this principle can also take place when an individual collects additional access privileges over time. This generally takes place when employees' job duties change or they are promoted to a new position or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary.

Physical

Physical controls observe and manage the environment of the work place and computing facilities. They also observe and manage access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks etc. Separating the network and work place into functional areas are also physical controls.

An important physical control that is not taken care of is the separation of duties. Making duties separate ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator – these roles and responsibilities must be separated from one another.

Defense in depth

Information security must be able to prevent the information from unauthorized access throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected in both states while in motion and while at rest. Throughout its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems. There are multiple ways the information and information systems can be threatened. If we want to protect the information completely during its lifetime, each component of the information processing system must have its own protection mechanisms. Defense in depth is way of building up, layering on and overlapping of security measures. The strength of any system is no greater than its weakest link. Using a defence in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in- depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people the next outer layer of the onion and network security, host-based security and application security forming the outermost layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense–in-depth strategy.

Security classification for information

An important part of information security and risk management is identifying the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label and list the required security controls for each classification.

Some factors that play major role in classifying about what information should be assigned included and how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. While classifying information Laws and other regulatory requirements are also important considerations.

The type of information security classification labels selected and used will depend on the nature of the organisation, with examples being:

- In the business sector, labels such as: Public, Sensitive, Private, Confidential.
- In the government sector, labels such as: Unclassified, Sensitive But Unclassified, Restricted, Confidential, Secret, Top Secret and their non-English equivalents.
- In cross-sectoral formations, the Traffic Light Protocol, which consists of: White, Green, Amber and Red.

Training must be provided to all employees in the organization, as well as business partners, on the classification schema and understanding the required security controls and handling procedures for each these classification. The classification a particular information asset has been assigned should be examined from time to time to make sure the classification is still appropriate for the information and to make sure that the security controls required by the classification are in place.

Access control

Only the people who Are authorized to access the protected information should access the information. The computers must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected - the more sensitive or valuable the information the stronger the control mechanisms need to be. The fundamentals on which access control mechanisms are based on identification and authentication.

Identification is an assertion of who someone is or what something is. If a person makes the statement “Hello, my name is John Doe” they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe.

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe (a claim of identity). The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be.

There are three different types of information that can be used for authentication: something you know, something you have or something you are. Examples of something you know include such things as a PIN, a password or your mother’s maiden name. Examples of something you have include a driver’s license or a magnetic swipe card. Something you are refers to biometrics. Examples of biometrics include palm prints, finger prints, voice prints and retina (eye) scans.

Strong authentication requires providing information from two of the three different types of authentication information. For example, something you know plus something you have. This is called two factor authentication.

If we look at the computer systems today, the Username is the most common form of identification and the Password is the most common form of authentication. Though usernames and passwords are important and are used still they are insufficient.more and more sophisticated mechanisms are replacing the usernames and passwords.

Once a person, programme or computer has successfully been identified and authenticated then it must be examined what informational resources they are allowed to access and what actions they will be allowed to perform (run, view, create, delete or change). This is called authorization.

Authorization to access information and other computing services begins with administrative policies and procedures. The policies describe that what information and computing services can be accessed, by whom and under what conditions. The access control mechanisms are then configured to enforce these policies.

Different computing systems have different types of access control techniques – some may even offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The non-discretionary approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The discretionary approach gives the creator or owner of the information resource the ability to control access to those resources. In the Mandatory access control approach, access is granted or denied basing upon the security classification assigned to the information resource.

Examples of common access control mechanisms in use today include Role-based access control available in many advanced Database Management Systems, simple file permissions provided in the UNIX and Windows operating systems, Group Policy Objects provided in Windows network systems, Kerberos, RADIUS, TACACS and the simple access lists used in many firewalls and routers.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies make sure that the people are held accountable for their actions. All failed and successful authentication attempts must be logged and all access to information must leave some type of audit trail.

Cryptography

Cryptography is used by information security to convert usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been converted or encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is a process used in information security to prevent the information from unauthorized or accidental disclosure while the information is being transmitted and while information is in storage.

Cryptography in information security has other useful applications which include improved authentication methods, message digests, digital signatures, non-repudiation and encrypted network communications. Application which are older such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure)

WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and E-mail.

Cryptography is not the solution for information security it may also have security problems when they are not correctly implemented. Cryptographic solutions should be implemented with industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. We should also take care of length and strength of the encryption key. A short key will produce weak encryption. The encryption keys used should be kept secure with the same degree of rigor as any other confidential information. They must be protected from people who are not authorized to use and from disclosure and destruction and they must be available when needed. PKI solutions address many of the problems that surround key management.

Check Your Progress 3

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Write a note on enterprise information security architecture.

....

....

....

....

....

2) Write a note on information security professionalism.

....

....

....

....

....

3) What do you understand by defense in depth?

....

....

....

....

....

4) Write a note on cryptography.

....

....

....

....

....

are older such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and E-mail.

Cryptography is not the solution for information security it may also have security problems when they are not correctly implemented. Cryptographic solutions should be implemented with industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. We should also take care of length and strength of the encryption key. A short key will produce weak encryption. The encryption keys used should be kept secure with the same degree of rigor as any other confidential information. They must be protected from people who are not authorized to use and from disclosure and destruction and they must be available when needed. PKI solutions address many of the problems that surround key management.

3.14 SUGGESTED READINGS

- http://intrepidusgroup.com.
- http://prismintl.org.
- http://searchsecurity.techtarget.com/.
- http://www.bangor.ac.uk1.
- http://www.sans.org.
- www.bsi-emea.com.

UNIT 4 LEGAL AND ETHICAL ISSUES

Structure

4.0 INTRODUCTION

In business the role of ethics can not be ignored. As we talk about ethics, the legal issues also can not be ignored in business. This unit covers the legal and ethical issues with respect to business perspective especially an online business. Reader will be able to learn about the important facts to a business successfully and honestly.

4.1 OBJECTIVES

After studying this unit, you should be able to learn about:

- security of sensitive business information;
- legal and ethical issues of business world;
- ethical issues at work place;
- law for pregnant women;
- effect of gender discriminations;
- business security policies, procedures;
- issues of Internet marketing; and
- issues of e-commerce.

4.2 SECURITY DISCIPLINES TO SAFEGUARD SENSITIVE BUSINESS INFORMATION

Confidentiality is the term refer as the ethical and professional duty which is performed on not to disclose any inappropriate information to a third party. Certain professionals who hold Certified Confidentiality Officer (CCO) certification apply for the confidentiality because of their legal or ethical requirements. In business, it is used to protect the privacy of a business entity and its critical or sensitive business information. Policies and procedures are must for protection against spying and for intentional or unintentional disclosure of sensitive or owner's information. These policies and procedures are being mandated by laws or regulations or by the professional ethical obligations of employees. These policies and procedures are also being implemented as a best practice to avoid insider or outsider access to critical business information.

Inefficient preplanning of the flow of confidential and private information within the business organization may result in false safeguarding of critical business secrets and thefts of intellectual property which includes property protected by copyrights, trademarks and patents. A confidentiality audit is a crucial step to business's minimum requirements of being protected against danger or loss. This is a fact-finding, non-fault-finding audit that involves:

- A search for vulnerabilities through information collection and analysis and
- A way to identify leaks, sources and indicators potentially exploitable by an adversary

Reasons why business confidentiality can be important

- To keep Trade secrets and intellectual property away from business competitors.
- The improper dissemination of information about current business objectives or future projects may harm the business.
- For employee security and for the security of their families.
- For Job security.
- It encourages employees to make use of services which are being created to help them, such as counseling or other employee assistance programmes.
- It makes easier for the people to get help without any fear or damage to reputation or other relationships.

Confidentiality is based on four basic principles

1) Respect for a business's right to privacy.
2) Respect for human relationships in which business information is shared.
3) Appreciation of the importance of confidentiality to both the business and its employees.
4) Expectations that those who pledge to safeguard confidential information will actually do so.

Confidentiality is must for the great interests of the organization because disclosure of the information will cause great damage to the business or to other organizations.

The confidentiality exists when information is designated as "confidential" (e.g. stamped or announced). It also applies where the need is obvious or evident (depending on the nature of the material or context of the situation) or when needed by applicable law-even when the information is not so important.

It does not depend solely on the individual to determine what is confidential or not. If the organization treats the information as confidential, then the officials and employees of that organization must understand the need for confidentiality. Also these individuals are not permitted to disregard their duty to maintain confidentiality.

It is the duty of the Business officials and employees to keep certain business and personal information confidential. However this legal obligation exists even if officials and employees have not signed contracts or other documents related specifically to confidentiality.

Board members are being trusted and it is their fiduciary duty to honor the business's need to keep certain information confidential.

A Board member or employee who discloses confidential information can create significant legal liability for the organization if he/she is legally required to maintain confidentiality and may face personal liability in disclosing confidential information.

10 postulates about confidentiality in the business world

The first postulate says that a dynamic security mechanism is required to prevent losses (loss = cost) that will help to achieve objectives, i.e. the continued smooth operation of the business while ensuring:

- The security of both tangible and intangible elements of business.
- The security of employees and materials.
- The security of information, communications and information systems that are used to manage risk (risk = intention + ability + opportunity), whether the risk is personal, human, physical, technological or other has a great impact on the well being of the organization.

The second postulate says that these security mechanisms must involve:

- Prevention
- Tracking
- Corrective actions.

The third postulate says that the security mechanism need real-time exposure and the tactical assessments that have been taken into account are:

- The risk or threat to the whole business;
- The acceptable level of risk or threat;
- The processes of reacting to a threat;
- The need to reduce the overall vulnerability.

The fourth postulate says that the security mechanism must specially address the following policies and procedures to produce effective and tangible results.

- Policies for how to implement the security mechanism;
- Procedures detailing the implementation process.

The fifth postulate is to integrate the above issues in a coherent programme, call the "Security Programme" or "Security Master Plan".

The sixth postulate says that the current business risks linked to each other, create a complex co-dependency. Therefore the management of initial frontline responses (e.g. guard actions and responsibilities at a building entrance) has passed into the arena of comprehensive security management.

The seventh postulate says that the security strategy must determine the nature of risk in detail, in addition to specifying the response plan.

The eighth postulate says that the security mechanism must collect and spread information about security-related business processes as to manage the flow of information and the reputation of the business.

The ninth postulate says that if security mechanism become effective has to analyze recruiting information from different sources and use this information to protect the business.

The tenth postulate says that the security mechanism must be planned-in advance-to analyze what happens on the next business day after a serious adverse event. Crisis do not get anticipated or managed the vast majority of organizations and institutions once they occurred.

Crisis and Continuity

Business crisis interrupts the way an organization manage business and attracts significant news media coverage and/or public scrutiny. These crisis are the forces that produce risk for the economics and well-being of the organization and its employees.

Most of the business crisis such as loss of critical/sensitive business information, either sudden or chronic, depends on the amount of advance notice and the chain of events in the crisis. These risks are rising continuously in domestic, foreign and private sectors.

Sensitive Information Risk Analysis (SIRA) and Evaluation of Sensitive Information (ESA) is used by the business continuously to reduce and manage the risk of spying. The developed rules, policies, procedures, audits and continuing assessments are implemented to avoid the competitive loss of business secrets and is an important part of the overall framework of security.

Confidentiality is referred to as a stand-alone process which helps to identify complete pathways that links to a potential "window of opportunity". Conservative assumptions can also be useful to estimate business exposure based on indicators and facts. The other important element is to gain support and commitment to the process from the organization's executive management.

Confidentiality is prerequisite in any internal or external business transaction. A Certified Confidentiality Officer (CCO) can help and provide specific knowledge to avoid loss, to protect critical/sensitive business information, to safeguard proprietary information and to enrich a business's awareness and training on confidentiality issues. A CCO can also integrate into philosophy of organization and recommends the idea that the "Nothingness Treaty" (nothing happened yesterday, nothing happened today, nothing will happen tomorrow) is a poor philosophy for protecting an organization and its employees.

4.3 LEGAL, ETHICAL AND REGULATORY ISSUES

The Internet has reduced the geographic boundaries which help the organizations to conduct extensive research and planning to enter the e-commerce arena. Internet technology has a great effect on the global trade which includes multitude of products and services. E-Marketing tools used by the online travel industry helps the consumers to purchase travel services in convenient manner. However, many businesses and consumers are still worry of conducting their business over the Internet because of the shortfall of the predictable legal environment governing transactions. This paper will address the legal, ethical and regulatory issues for an e-commerce company and will focus on site security, confidentiality and international issues of Expedia, Travelocity and Orbitz.

Security, Confidentiality and International Issues

The global market is vast having no unified regulatory guidelines or standards. Due to which e-commerce businesses must implement varied contingencies to ensure compliance with both domestic and foreign tax requirements regarding the sale of products ad services. In the United States, firms are required to disclose any potential tax liabilities under the Sarbanes-Oxley Act of 2002, however there is no clear legislation of how state tax sales will be structured through e-commerce venues. In a polar opposite to the United States the European Union, issued a directive requiring "companies outside of the European Union to start paying value added tax on sales of electronically delivered goods and services to European customers" (Meller, 2002). Different national perspective regarding taxes requires individual e-commerce businesses to understand the global market and to develop internal controls to comply with the governing tax structure applicable to the areas in which they operate. In addition to tax concerns, U.S. firms must satisfy compliance with consumer protection and privacy legislation aimed at protecting individual consumers. For example, the Gramm-Leach-Bliley Financial Modernization Act requires company's to provide an option for consumers to determine if they want their information shared with third parties; the Children's Online Privacy Protection Act (COPPA) Rule which applies to commercial web sites operators and an online services directed to children under age 13. The law makes parents to control the information that is being collected by their children online and how such types of information are used by them. (FTC, 2006) Industry practices of web developers in the United States, Canada and Europe were studied by the Federal Trade Commission (FTC). In a FTC report to Congress "four widely accepted fair information practices regarding the collection of personal identifying information from or about consumers online are Notice, Choice, Access and Security." (FTC, 1998) FTC guidelines help the consumer-orientated commercial Web sites to adopt four widely accepted information practices:

1) **Notice** – Web sites would provide clear and conspicuous notice of their information practices to the customers, including what information they collect, how they collect it (e.g. directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access and Security to consumers, whether they disclose the information collected to other entities or whether other entities are collecting information through the site.

2) **Choice** – Web sites would offer choices to consumers to analyze them that how their personal information is being used beyond the use for which the information was provided (e.g. to consummate a transaction). Such choice would include both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

3) **Access** – Web sites would offer consumers reasonable access to the information which has been collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.

4) **Security** – Web sites would take reasonable steps to protect the security of the information they collect from the customers (FTC, 1998). The global marketplace has provided web-based firms with a larger customer community. However, charting the diverse domestic and international regulatory requirements will remain a challenge as independent nations develop legislation to regulate this medium.

Expedia

Expedia is very much concerned with security and privacy of its customers. According to Expedia's privacy policy, the company states "We understand that making purchases online involves a great deal of trust on your part; we take this trust very seriously and make it our highest priority to ensure the security and confidentiality of the personally identifiable information you provide us" (Expedia, 2006). In September of 2000, Expedia announced the successful completion of a privacy audit that was conducted by Pricewaterhouse Coopers. This audit took Expedia's to an extensive inspection of its business practices and how it relates to the organization's privacy policy (Expedia, 2000). Expedia's privacy policy explains how the organization handles customer data, the confidentiality in which customer information is handled and how the company secures this information. Expedia.com has also setup regional offices that work with specific geographic locations across the world. Each local site reflects the laws and issues of that specific area. Every regional site has its own version of Expedia's privacy policy and lists specific laws that apply to that country or area in which Expedia does business.

Travelocity

Security is Travelocity's top priority which protects consumer personal information through security protocols within the company's system infrastructure. Throughout the booking process, Travelocity ensures multiple security precautions after you completed your transactions. Firewall that act as shields to our computer networks makes the Travelocity systems very much protected. Travelocity ensure the protection of consumer's credit card transactions and encrypts the consumer financial and personal data residing in these systems.

Travelocity also shows concern about Privacy and confidentiality. Only third party travel service providers get the personal information when consumers reserve or purchase travels services through Travelocity Business. Customer private profile information is not sold to third parties. Occasionally, Travelocity Business will provide consumer information to a third party acting on their behalf for specialized projects such as market research surveys and contest entry processing .

International issues and global barriers help the Travelocity to improve its infrastructure to provide support to global pricing and taxation by its leveraging parent company Sabre's back-end system, which already ensures proper handling of international pricing. These improvement make Travelocity to offer services to customers in 94 countries. (Goodridge E, 2000).

Orbitz

Physical, administrative and technical safeguards are employed by Orbitz to protect the confidentiality and integrity of consumer information in its databases and reduce the risk of loss, misuse, unauthorized access, disclosures or modification of personal information. Any information transmitted electronically via the World Wide Web might not be secure. Orbitz makes the company to assume no liability for the loss of any information transmitted via the World Wide Web. However, personal financial data on credit cards used when making a booking, reservation or purchase on the site is encrypted for the transaction

Orbitz's privacy policy tells that consumer privacy is of great importance. Their privacy policy explains the principles and practices that apply to the Information collected from users which are personal in nature for services on the company site, in telephone or e-mail communications or in interviews, surveys, sweepstakes, contests or raffles. Simple put, without the consumer's knowledge and permission Orbitz will not collect their Personal Information; nor disclose their Personal Information to third parties. Orbitz will make customers to view, correct or remove their Personal Information; and allow to takes reasonable steps to protect the

Personal Information

the international issues associated with Orbitz are managed by Travelport. Travelport solutions are a subsidiary of Cendant Corp. provides a global full service of strategic services and tools for mid and large corporations, providing access to online booking tools and global distribution services. Travelport's International Rate Desk specializes in faring complex, multi-segment international itineraries. Using their experience and knowledge of customer contracts, specialized agents find the best options for international travelers-and average savings of $550 per ticket (Cendant Corporate Travel, 2004).

Research and planning must occur when an organization decides to enter into e-commerce, because the Internet has changed the way organizations do business; these organizations must understand the legal, regulatory and ethical considerations of e-commerce before commencing an online website. A company could risk its success and livelihood by not abiding by the law or allowing private information or data to become compromised. Expedia, Travelocity and Orbitz, e-commerce sites do business in international markets and have addressed these issues by working with local countries and regions on how to best address the regulations of their respective geographic areas to ensure that each is compliant and is acting within the local laws.

Check Your Progress 1

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Why business confidentiality is important?

....

....

....

....

....

2) Write four basic principles on which confidentiality is based upon.

....

....

....

....

....

3) Write a note on crisis and continuity.

....

....

....

....

....

4) What are four widely accepted information practices?

....

....

....

....

....

4.4 ETHICAL ISSUES AND EMPLOYER MONITORING INTERNET USAGE

Internet monitoring put employers and employees at odds in the workplace because both are trying to protect personal interests. Employees want to maintain privacy and the employers want to ensure company resources not to be misused. Companies are trying to maintain ethical monitoring policies by avoiding indiscriminate monitoring of employees' online activities.

Function

Some employers keep eye on the Internet use in the workplace area to protect their companies from legal problems that could arise if employees of the company misuse its computers for illegal online activities. Other employers measure the decline in productivity as some of the workers use the Internet to handle their personal business on company working time. The ethical challenges that are being faces by the company involve protecting their interests by monitoring the Internet while ensuring sense of privacy at the workplace.

Company Policies

Companies while monitoring workers' Internet may install software on their computers to block access to specific sites that are unrelated to their jobs. A "PC World" article by Tony Bradley indicates that employers can establish respect for employees' privacy by creating a written policy that clearly defines acceptable uses for company computers. The policy outlines the results for violating the policy and also the company's right to monitor Internet users. Bradley notes that Internet monitoring could be a breach of privacy if employees never receive written notice on the appropriate use of company computers and the employer's right to monitor online activities

Company Rights

Some employees who fought against Internet monitoring in the workplace have tried to use the Fourth Amendment of the U.S. Constitution to support their case, according to Bradley. They claimed that Internet monitoring violates the Fourth Amendment because it is equal to an illegal search and seizure of property. Bradley also indicates that courts took side of employers, determining that employers own their company computers and related resources. Therefore, employers have the right to monitor the use of their property to guard companies against illegal activities.

Considerations

The Nolo law information website recommends that the Employers keep themselves on fine ethical and legal grounds by monitoring only Internet use for business-related reasons For example, you may walk by an employee's desk and notice a game site on the employee's computer monitor however you would be able to analyze that employee is wasting company time by playing online games.

4.5 LIST OF ETHICAL AND LEGAL ISSUES WHEN ADVERTISING

The advertising industry operates through strict regulations and is monitored by the legal agencies. Even having truth-in-advertising laws, advertisers have significant leeway to violate the ethical standards of a wide range of consumers. Advertisers have to take extra care when advertising to children, advertising potentially harmful products and using psychological tactics to stimulate demand. It helps to craft legal, responsible ad messages.

Truth in Advertising

The advertisements must be truthful not deceptive and unfair. The Evidences must be available for the advertisers for the back up claims. The FTC defines deceitful statements that are likely to misguide consumers who act reasonably under normal circumstances and that will affect purchase decisions of consumers. Unfair advertisements are proved to cause substantial, unavoidable injury while using a product, unless the injury is overcome by benefits.

Advertising to Children

Social development can impede or develop negative self images in children while building brand loyalty in them before they even understand what a brand is about. However the best way to act ethically in this area is to advertise to parents, not children.

Advertising Harmful Products

Different countries have different perception for advertising vice products and services and maintain a balance between placing personal responsibility on citizens and regulating what citizens are allowed to indulge in. For example, cigarette advertising is only permitted on specific media, excluding television and radio, while alcohol advertising is allowed on all media. Companies have to take a good look at the true nature of their product lines when deciding whether they are acting ethically as advertisers. Television ads for fast food hamburgers are completely legal and effective at building demand, for example, but doctors in the 21^{st} century are beginning to find links between fast food and a national obesity epidemic. Pharmaceutical ads with lists of side effects, as another example, are often followed 10 years later by attorneys' ads for class-action lawsuits against the companies for wrongful injury.

Advertising Tactics

Advertising tactics present more ethical challenges. Advertisers have a range of less-than-ethical yet legal tools at their disposal, including subliminal advertising, emotional appeals, taking advantage of less educated individuals, spreading propaganda for political campaigns and other tactics ethical advertisers consistently refrain from using. At the end we only can say that consumers will be more attracted to companies that do not use underhanded, psychologically manipulative tactics to gain their business.

4.6 HOW TO HANDLE ETHICAL ISSUES AT THE WORKPLACE?

Morality and values-based dilemmas are difficult to handle at workplace when employees have to choose right or wrong according to their own principles. Forward thinking employers are able to handle potential conflicts and implement ethical policies that arise due to different types of opinions, values and culture at the workplace. However, it requires a steady and cautious approach which can be dangerous or illegal to such matters.

Step 1

Develop a policy at workplace which is based on your company's philosophy, its mission statement and code of conduct. Incorporate the policy into your performance management programme to uphold professional standards throughout the employees' job performance and interaction with peers and supervisors, providing copies of the revised handbook to employees. Getting signed the acknowledgement forms from employees that indicate they received and understand the workplace ethics policy.

Step 2

Provide workplace ethics training to employees. Provide different instruction methods to employees to make them learn as how to address and resolve ethical dilemmas. An effective way to facilitate the ethical training at workplace is Experiential learning or role-play. Examples consists of scenarios which include the misappropriation of company funds, personal values related to improper workplace relationships and the organization's compliance with regulatory controls.

Step 3

Designate an ombudsperson in charge of handling employees' who helps in considering whether your organization needs an ethics hotline or not, an ethics hotline is a confidential service through which employees may contact whenever they encounter workplace dilemmas that make them uncomfortable or in threatening positions. Confidential hotlines are an effective way to assure employees' anonymity, which are considered as "whistle blowing" actions.

Step 4

Whistle blowing pertains by Research federal, state and municipal labor and employment laws. Refrain from making employment decisions, such as termination or suspension, in connection with whistle blowing. Seek legal advice for employee reports of workplace ethics issues that increase your organization's liability under federal, state or municipal employment law. Under the Texas Whistleblower Act, for example, public-sector employees may be entitled to damages if an employer engages in retaliatory actions based on an employee who, in good faith, files a complaint related to workplace ethics. The Act grants "public employee who claims that his suspension, termination or other adverse personnel action was in retaliation for his good faith reporting of violations of the law the right to sue for damages and other relief."

Step 5

Applying workplace policy in consistent manner while addressing workplace issues and concerning employee about workplace ethics. Communication with the same expectations for all employees – whether they are in executive positions or front-line production roles – and approach every issue with equal interpretation of the company policy.

4.7 HOW DO ETHICS MAKE YOU A BETTER PERSON AT THE WORKPLACE

Ethical employees are those who make decisions for their employers, co-workers and outside stakeholders in addition to themselves. Workplace ethics center on such diverse issues as discrimination, fraud, theft and personal politics. Ethical employees are actually more financially valuable to their employers and more valued by co-workers and peers. Understanding how ethics can make you a better person in the workplace is a solid starting point to do the right thing.

Trusting Relationships

Ethical employees build trust in their workplace relationships, helps people to open up to them, share private information and feel more at ease communicating with them. Areas that affect trust include honesty, fairness and avoiding rumors. Gaining the trust of your co-workers can enhance your productivity by making it easier for you to communicate and work with others in the workplace. Employees who spread distrust can meet resistance when seeking help from others, but trusted co-workers can always find a helping hand. Gaining the trust of your managers can open doors for new responsibilities at work.

Team Cohesiveness

The ethical commitments of individual employees have an effect on team and department performance in addition to individual performance. Being an ethical employee makes you a better team player, always making positive contributions in group settings and never hindering group progress. An employee who is stealing from company funds, for example, can cause divisions, rumors and resentment among accounting employees as co-workers begin to suspect others of participating. An employee with a solid commitment to ethics can identify and expose issues of theft early.

Companies live or die on the trust they place in their employees. An unethical employee in the ranks can land an entire company in legal trouble or can destroy a company's hard-earned reputation in the marketplace. Ethical employees are better people to have working for any company, as top managers and business owners can rest assured that their employees adhere to ethics policies and use ethical reasoning when making company decisions.

Personal Wellness

Being an ethical employee makes you a better person while increasing your value to others. Unethical acts such as theft and fraud, for example, can weigh people down with guilt and paranoia, resulting in hostile and fearful attitudes at work and at home. Employees who spread false rumors or lies about others can live in a constant state of paranoia, as another example, as they try to remember which lies they told to whom and when. Using ethics to guide all of your decisions at work can grant you peace of mind, emotional stability and the ability to cultivate lasting friendships. This can increase your job satisfaction, in addition to giving you more serenity for life in general.

Check Your Progress 2

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Write a note on company policies and company rights.

....

....

....

....

....

2) Write a note on advertising tactics.

....

....

....

....

....

3) How can we build trusting relationships at the work place?

....

....

....

....

....

4) Discuss the importance of personal wellness in the work place.

....

....

....

....

....

4.8 LAW FOR PREGNANT WOMEN AT THE WORKPLACE

Federal law placed several protections that stops employers to discriminate pregnant women. For instance, employer health insurance plans must treat pregnancies like other medical conditions. However, some legal protections for pregnant women depend on the size of the company in which they work.

Family Leave Act

The Family and Medical Leave Act (FMLA) allows pregnant women to take up to 12 weeks of unpaid leave from their jobs for the birth and care of a newborn. However, some women who work for small companies are not able to take advantage of FMLA benefits. The law is only applicable to companies which have 50 or more employees. Furthermore, employees aren't eligible for FMLA if they have not worked for at least 12 months in that company having a working experience of 1250 hours.

Pregnancy Discrimination Act

The Pregnancy Discrimination Act is an amendment to Title VII of the Civil Rights Act of 1964. According to the Equal Employment Opportunity Commission this law stops employers from neglecting them to hire a woman because of her pregnancy. The EEOC also describes that employers must treat a pregnant employee the same as they treat other disabled workers.

Furthermore, employers must allow pregnant women to work as long as they want if they can perform their job duties.

Health Insurance

Pregnant employees also get health insurance protections under the Pregnancy Discrimination Act. For instance, employers who provide health insurance for workers must cover expenses for pregnancy-related conditions under the same terms as other medical conditions. Insurance providers are also not able to charge workers larger deductibles solely to cover pregnancies.

Benefits and Complaints

Temporary disability rules also help to protect pregnant employees regarding fringe benefits. For example, the Pregnancy Discrimination Act makes employers to treat pregnant women the same way as they treat other temporarily disabled employees while calculating vacation time or awarding pay increases. According to the EEOC, Employees are free to charge a pregnancy discrimination charge against an employer. The law also provides protections to employees who choose to participate in a discrimination investigation.

4.9 EFFECT OF GENDER DISCRIMINATION AT THE WORKPLACE

Gender discrimination causes many negative effects on victims and businesses.

According to TNS Research Surveys, 68 percent of women are suffering from gender discrimination in the workplace. The Federal law protects these women and others from discrimination in the work place. The Equal Pay Act of 1963 dissolves the practice of paying men more than women even on performing the same jobs and duties. In 1964, the Civil Rights Act provided this protection to other minorities. Despite of these, many women still suffer from gender-based discrimination in some businesses.

Lost Productivity

The Victims lose motivation and morale which is required by them to perform their jobs effectively. According to a report written by Jodi L. Jacobson of the World Watch Institute, gender bias also leads to loss in productivity. Things that may lead to this loss of morale and motivation could include jokes about an employee's gender that imply inferiority, offensive jokes of a suggestive or sexual nature and jokes implying that an employee’s work is sub-par due to his or her gender. Federal law bans this type of workplace harassment, by superiors or coworkers.

Promotions

Stereotypical views regarding gender can make supervisors to get into the illegal practice of making a person over for promotion due to gender. While this can happen to both genders, but mostly women get pass over for promotion due to preconceived notions about their roles and abilities. For example, a fire chief may repeatedly pass over a female fire fighter for promotion, due to resentment stemming from women applying to the force or due to a belief that men inherently perform better in these positions. Supervisors may pass over qualified males for promotions in industries that employ a high percentage of women compared to men, such as teaching positions or those industries involving care of children.

Family Responsibilities

Women who have young children at home have to face push-back when interviewing due to their family responsibilities. the law does not allow a prospective employer to ask about family responsibility outright, but it often comes out during the interview process anyway. This may make the hiring manager to pass over a qualified female candidate if he feels she will be torn between her home and job responsibilities. If the woman makes it into the position, her supervisor can view her employee file to see that she has young children signed up on insurance or other benefits. He then may choose to give her less responsibility or assign menial tasks to her that do not fit her job description. This type of practices still exists in companies.

Destruction

Those who discriminated may feel such strong resentment and loss of self worth that they resort to destruction as a way to get back at the discriminatory employer or coworkers. Destructiveness may manifest as physical violence against others, destruction of property or propagation of malicious rumors about people in the company.

4.10 BUSINESS SECURITY POLICIES AND PROCEDURES

With much of the business world running on computer networks, it is not important for companies to build security into their networking infrastructures. Security policies are an important part of the business world today and it is important that every member of the executive staff and management team understand the importance of keeping data safe and secure.

Know the Threats

It is important to keep in mind that most data loss comes not at the hands of organized bad guys but also from inside the network. Sometimes the damage is malicious in nature, but other times the data gets lost when technically unsophisticated employees accidentally delete files or download harmful programmes. Understanding the area of threats will help you fight back with the right security policies and procedures. One of the effective step network administrators has to take is to apply a global security policy that stops users from downloading software or running executable programmes. Exceptions to this policy can be made on a case-by-case basis.

Watch Out for DOS

Today many modern computer users are not familiar with the history of DOS. However, some employees may know just enough in this area that hiding the DOS window or restricting its use can be a smart move. With this, employees could delete files that Windows would otherwise not allow to be deleted, including files that are needed for the proper operation of the PC. Simply restricting the use of the DOS window can save network administrators a lot and overcomes the chances of important data to get lost.

Restrict the Use of the Run Dialog Box

Simply clicking the Start button and choosing Run from the menu can give your users access to an almost unlimited number of commands--including some commands they should not be running. By clicking Start and Run, users can edit the registry, run executable programmes and much more. Since most ordinary users have no compelling reason to use these features, restricting the use of the Start/Run dialog box can be a very good thing. Removing the ability to use this powerful but potentially dangerous tool is one way to keep your network--and your valuable data--safe from harm.

4.11 INTERNET MARKETING ETHICS ISSUES

The internet marketing or advertising ethical issues have great importance. The ethics are the cultural values of the society. It is the internet marketing in a society where legal and ethical limits are pushed to the maximum The Internet is a growing and a continually evolving creature that will live on in perpetuity. As such, it would be wise to ponder the e business legal and Internet marketing ethical issues.

Whatever is written and published online will be there forever. Imagine the billions of pages that are and will be stored for a long time. There is even a site where you can go Way Back to check out the history that is not in use of other websites and view pages that were created at the beginning. Video, films, movies and audio in various applications formats are also viewable. Security and privacy concerns along with e-business regulatory issues become more prevalent.

It will be more difficult to analyze whom to trust online including all the unethical, illegal and Internet marketing and online advertising frauds and E-business e-mail scams.

Also consider carefully what is published on blogs for short. A blog is simply a website in which people share their daily, weekly or monthly personal or corporate thoughts, ideas and happenings with others. When dealing with ethics in a B2B company and B2C clients a major degree of trust and responsibility is being imparted to a person or group that maintains the Web site. Electronic copyright, e-commerce, credit/cash policies, international trade, tariffs, privacy, digital media offers and security are a few of the items to be considered.

Importance of Ethics on the Internet

Using good ethical standards in online world reflects your business directly online and affects all aspects of your business. It affects your company's brand image and subsequently how sales, marketing and advertising principles are applied to the task of making your company profitable for the long period of time. It also affects your employees and how they represent your company online, on the phone, in person and all types of customer service and customer relations when dealing with buyers, engineers, sales leads and potential customers in both the business of B2B AND B2C both of which covers the majority of business types in the world.

4.12 E-COMMERCE ETHICAL AND LEGAL ISSUES

The vast use of Internet advertising provides a solid platform for Electronic Commerce (or e-commerce) to explode. E-Commerce provides secure shopping transactions coupled with instant verification and validation of credit card transactions

E-commerce is a technological innovation which is followed by frequent incorporation of ethical standards into law. New forms of E-Commerce enables new business practices with many advantages but also bring numerous risks. Let's discuss about the ethical and legal issues related to e-business.

Ethical issues

In general, many ethical and global issues of Information Technology applied to e-business. So, what are the issues particularly related to e-commerce like

Web tracking

E-businesses provide information that how visitors use a site through log files. Analysis of log file consists of turning log data into application service or installing software that can pluck relevant information from files in-house. Companies track individual's movement through tracking software and analyzing cookie. The tracking history is stored on your PC's hard disk and any time you revisit a website, the computer knows it. Many smart end users install programmes such as Cookie cutters, Spam Butcher, etc which can provide users some control over the cookies.

The battle between computer end users and web trackers goes on with a range of application programmes. For example, software such as Privacy Guardian, My Privacy, etc can protect user's online privacy by erasing browser's cache, surfing history and cookies, detecting and removing spyware programmes like Ad-Aware are present. A data miner application, SahAgent collects and combines Internet browsing history of users and sends it to servers. The battle goes on!

Privacy

The Electronic Payment Systems knows identifies the buyer so it becomes necessary to protect the identity of a buyer

A privacy issue is related to the employees of company who are tracked by the Monitoring systems installed to monitor e-mail and other web activities in order to identify those employees who extensively use business hours for non-business activities. The e-commerce activities performed by a buyer can be tracked by organizations. For example, reserving railway tickets for their personal journey purpose can be tracked. Many employees don't want to be under the monitoring system even while at work.

E-Commerce puts brokers and some of the company employees in danger zone and results in elimination from their jobs.

Disintermediation and Reintermediation

Intermediation is one of the most important and interesting e-commerce issue related to loss of jobs. The services provided are

1) Matching and providing information

2) Value added services such as consulting

The first type of service (matching and providing information) can be fully automated and this service is likely to be in e-marketplaces and portals that provide free services. Where as the value added service requires expertise and this can only be partially automated.

The brokers who provide value added services or who manage electronic intermediation (also known as info mediation), are not only surviving but may actually prosper and this phenomenon is called Reintermediation.

Disintermediation has adverse affect on the traditional sales channel. The new opportunities for reintermediation includes services required to support or complement e-commerce The factors that should be considered here are the enormous number of participants, extensive information processing, delicate negotiations etc. They need a computer mediator to be more judgemental.

Legal issues

Internet fraud and its sophistication have been grown even faster than the Internet itself. There is a chance of a crime over the internet when buyers and sellers do not know each other and cannot even see each other. Many frauds were committed over the internet during the first few years of e-commerce as the public is the witness. Let's discuss the legal issues specific to e-commerce.

Fraud on the Internet

E-commerce fraud popped out with the rapid increase in popularity of websites. It is a hot issue for both cyber and click-and-mortar merchants. The swindlers are active mainly in the area of stocks. The small investors are lured by the promise of false profits by the stock promoters. Auctions are also conductive to fraud, by both sellers and buyers. The availability of e-mails and pop up ads has paved the way for financial criminals to have access to many people. Other areas of potential fraud include phantom business opportunities and bogus investments.

Copyright

The copyright laws protect Intellectual property in its various forms and cannot be used freely. It is very difficult to protect Intellectual property in e-commerce. For example, if you buy software you have the right to use it and not the right to distribute it. The distribution rights are with the copyright holder. Also, copying contents from the website also violates copy right laws.

Domain Names

One major legal issue is comprises of domain names. Internet addresses are known as domain names and as they appear in levels, top level domain names are assigned to non-profit organization which also checks for conflicts or possible infringement of trademarks. Problems arise when several same name companies fights over the same domain name. The problem of domain names was alleviated somewhat in 2001 after several upper level names were added to com.

Another issue to look out is Cyber squatting, which refers to the practice of registering domain names with the desire of selling it at higher prices. Security features such as authentication, non-repudiation and escrow services can protect the sellers in e-commerce.

One must be careful while performing e-commerce activities. The need to educate the public about the ethical and legal issues related to e-commerce is highly important from a buyer as well as seller perspective.

Check Your Progress 3

Note: a) Space is given below for writing your answers.

b) Compare your answers with the one given at the end of this Unit.

1) Discuss gender discrimination with respect to loss of productivity.

....

....

....

....

2) How can we enhance security by restricting the use of the Run Dialog Box?

....

....

....

....

3) Write a note on the importance of ethics on Internet.

....

....

....

....

4) Discuss the ethical issues with respect to e-commerce.

....

....

....

....

4.13 LET US SUM UP

This unit is an effort towards covering some of the important topics related to legal and ethical issues of business, especially with respect to online business. The reader will be able to learn about security disciplines to safeguard sensitive, legal, ethical and regulatory issues. Learner will also know about the ethical issues with respect to employer and employees perspective. Issues related with advertisement and topics like gender discrimination in the workplace are also covered. Finally the topics like business security policies and procedures, ethical and legal issues of e-commerce are also discussed.

4.14 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Business confidentiality is important for the following:

- To keep Trade secrets and intellectual property away from business competitors.
- The improper dissemination of information about current business objectives or future projects may harm the business.
- For employee security and for the security of their families.
- For Job security.
- It encourages employees to make use of services which are being created to help them, such as counseling or other employee assistance programmes.
- It makes easier for the people to get help without any fear or damage to reputation or other relationships.

2) The four basic principles on which confidentiality is based upon are the following:

   1) Respect for a business's right to privacy.
   2) Respect for human relationships in which business information is shared.
   3) Appreciation of the importance of confidentiality to both the business and its employees.

4) Expectations that those who pledge to safeguard confidential information will actually do so.

3) Business crisis interrupts the way an organization manage business and attracts significant news media coverage and/or public scrutiny. These crisis are the forces that produce risk for the economics and well-being of the organization and its employees.

Most of the business crisis such as loss of critical/sensitive business information, either sudden or chronic, depends on the amount of advance notice and the chain of events in the crisis. These risks are rising continuously in domestic, foreign and private sectors.

Sensitive Information Risk Analysis (SIRA) and Evaluation of Sensitive Information (ESA) is used by the business continuously to reduce and manage the risk of spying. The developed rules, policies, procedures, audits and continuing assessments are implemented to avoid the competitive loss of business secrets and is an important part of the overall framework of security.

Confidentiality is referred to as a stand-alone process which helps to identify complete pathways that links to a potential "window of opportunity". Conservative assumptions can also be useful to estimate business exposure based on indicators and facts. The other important element is to gain support and commitment to the process from the organization's executive management.

4) 1) **Notice** – Web sites would provide clear and conspicuous notice of their information practices to the customers, including what information they collect, how they collect it (e.g. directly or through non-obvious means such as cookies), how they use it, how they provide Choice, Access and Security to consumers, whether they disclose the information collected to other entities or whether other entities are collecting information through the site.

2) **Choice** – Web sites would offer choices to consumers to analyze them that how their personal information is being used beyond the use for which the information was provided (e.g. to consummate a transaction). Such choice would include both internal secondary uses (such as marketing back to consumers) and external secondary uses (such as disclosing data to other entities).

3) **Access** – Web sites would offer consumers reasonable access to the information which has been collected about them, including a reasonable opportunity to review information and to correct inaccuracies or delete information.

4) **Security** – Web sites would take reasonable steps to protect the security of the information they collect from the customers" (FTC, 1998). The global marketplace has provided web-based firms with a larger customer community. However, charting the diverse domestic and international regulatory requirements will remain a challenge as independent nations develop legislation to regulate this medium.

Check Your Progress 2

1) **Company policies and company rights**

Company Policies

Companies while monitoring workers' Internet may install software on their computers to block access to specific sites that are unrelated to their jobs. A

"PC World" article by Tony Bradley indicates that employers can establish respect for employees' privacy by creating a written policy that clearly defines acceptable uses for company computers. The policy outlines the results for violating the policy and also the company's right to monitor Internet users. Bradley notes that Internet monitoring could be a breach of privacy if employees never receive written notice on the appropriate use of company computers and the employer's right to monitor online activities

Company Rights

Some employees who fought against Internet monitoring in the workplace have tried to use the Fourth Amendment of the U.S. Constitution to support their case, according to Bradley. They claimed that Internet monitoring violates the Fourth Amendment because it is equal to an illegal search and seizure of property. Bradley also indicates that courts took side of employers, determining that employers own their company computers and related resources. Therefore, employers have the right to monitor the use of their property to guard companies against illegal activities.

2) Advertising tactics present more ethical challenges. Advertisers have a range of less-than-ethical yet legal tools at their disposal, including subliminal advertising, emotional appeals, taking advantage of less educated individuals, spreading propaganda for political campaigns and other tactics ethical advertisers consistently refrain from using. At the end we only can say that consumers will be more attracted to companies that do not use underhanded, psychologically manipulative tactics to gain their business.

3) Ethical employees build trust in their workplace relationships, helps people to open up to them, share private information and feel more at ease communicating with them. Areas that affect trust include honesty, fairness and avoiding rumors. Gaining the trust of your co-workers can enhance your productivity by making it easier for you to communicate and work with others in the workplace. Employees who spread distrust can meet resistance when seeking help from others, but trusted co-workers can always find a helping hand. Gaining the trust of your managers can open doors for new responsibilities at work.

4) Being an ethical employee makes you a better person while increasing your value to others. Unethical acts such as theft and fraud, for example, can weigh people down with guilt and paranoia, resulting in hostile and fearful attitudes at work and at home. Employees who spread false rumors or lies about others can live in a constant state of paranoia, as another example, as they try to remember which lies they told to whom and when. Using ethics to guide all of your decisions at work can grant you peace of mind, emotional stability and the ability to cultivate lasting friendships. This can increase your job satisfaction, in addition to giving you more serenity for life in general.

Check Your Progress 3

1) **Gender discrimination with respect to loss of productivity**

The Victims lose motivation and morale which is required by them to perform their jobs effectively. According to a report written by Jodi L. Jacobson of the World Watch Institute, gender bias also leads to loss in productivity. Things that may lead to this loss of morale and motivation could include jokes about an employee's gender that imply inferiority, offensive jokes of a suggestive or sexual nature and jokes implying that an employee's work is sub-par due to his or her gender. Federal law bans this type of workplace harassment, by superiors or coworkers.

2) **We enhance security by restricting the use of the Run Dialog Box**

Simply clicking the Start button and choosing Run from the menu can give your users access to an almost unlimited number of commands--including some commands they should not be running. By clicking Start and Run, users can edit the registry, run executable programmes and much more. Since most ordinary users have no compelling reason to use these features, restricting the use of the Start/Run dialog box can be a very good thing. Removing the ability to use this powerful but potentially dangerous tool is one way to keep your network--and your valuable data--safe from harm.

3) **Importance of ethics on Internet**

Using good ethical standards in online world reflects your business directly online and affects all aspects of your business. It affects your company's brand image and subsequently how sales, marketing and advertising principles are applied to the task of making your company profitable for the long period of time. It also affects your employees and how they represent your company online, on the phone, in person and all types of customer service and customer relations when dealing with buyers, engineers, sales leads and potential customers in both the business of B2B AND B2C both of which covers the majority of business types in the world.

4) In general, many ethical and global issues of Information Technology applied to e-business. So, what are the issues particularly related to e-commerce like

Web tracking

E-businesses provide information that how visitors use a site through log files. Analysis of log file consists of turning log data into application service or installing software that can pluck relevant information from files in-house. Companies track individual's movement through tracking software and analyzing cookie. The tracking history is stored on your PC's hard disk and any time you revisit a website, the computer knows it. Many smart end users install programmes such as Cookie cutters, Spam Butcher, etc which can provide users some control over the cookies.

The battle between computer end users and web trackers goes on with a range of application programmes. For example, software such as Privacy Guardian, My Privacy, etc can protect user's online privacy by erasing browser's cache, surfing history and cookies, detecting and removing spyware programmes like Ad-Aware are present. A data miner application, SahAgent collects and combines Internet browsing history of users and sends it to servers. The battle goes on!

Privacy

The Electronic Payment Systems knows identifies the buyer so it becomes necessary to protect the identity of a buyer.

A privacy issue is related to the employees of company who are tracked by the Monitoring systems installed to monitor e-mail and other web activities in order to identify those employees who extensively use business hours for non-business activities. The e-commerce activities performed by a buyer can be tracked by organizations. For example, reserving railway tickets for their personal journey purpose can be tracked. Many employees don't want to be under the monitoring system even while at work.

E-Commerce puts brokers and some of the company employees in danger zone and results in elimination from their jobs.

Disintermediation and Reintermediation

Intermediation is one of the most important and interesting e-commerce issue related to loss of jobs. The services provided are

- Matching and providing information
- Value added services such as consulting

The first type of service (matching and providing information) can be fully automated and this service is likely to be in e-marketplaces and portals that provide free services. Where as the value added service requires expertise and this can only be partially automated.

The brokers who provide value added services or who manage electronic intermediation (also known as info mediation), are not only surviving but may actually prosper and this phenomenon is called Reintermediation.

Disintermediation has adverse affect on the traditional sales channel. The new opportunities for reintermediation includes services required to support or complement e-commerce The factors that should be considered here are the enormous number of participants, extensive information processing, delicate negotiations etc. They need a computer mediator to be more judgemental.

4.15 SUGGESTED READINGS

- http://public.pacbell.net.
- http://smallbusiness.chron.com.
- http://www.eiu.edu.
- http://www.neiu.edu.
- www.orbitz.com.
- www.travelocity.com.

NOTE

MPDD-IGNOU/P.O. 1T/September, 2011

ISBN : 978-81-266-5565-6