UNIT 11 CYBER SECURITY MEASURES

Structure

11.1 Introduction

11.2 Cyber Security Measures

11.2.1 Role of cyber security analysts

11.2.2 Essential cyber security measures

11.2.3 Precautionary cyber-security measures enterprise takes

11.3 IoT and its Impact

11.4 Vulnerable Information on Internet

11.4.1 Vulnerabilities of Systems

11.4.2 Internet Vulnerabilities

11.4.3 Wireless Security Challenges

11.4.4 Malicious Software

11.4.5 Hackers and Computer Crime

11.4.6 Cyber Crime

11.4.7 Global Threats: Cyber terrorism and Cyber Warfare

11.5 Cyber Forensic

11.6 Securing the Business on Internet

11.7 Securing Network Transaction

11.8 Security Measures and Enforcement

11.8.1 Biometric Security Measures

11.8.2 Non-biometric Security Measures

11.8.3 Cyber Physical Security System

11.8.4 Access Control

11.8.5 Ensuring Software Quality

11.9 Let Us Sum Up

11.10 Keywords

11.11 Terminal Questions

11.0 OBJECTIVES

After studying this unit, you should be able to:

- understand various cyber security measures;
- explain about vulnerable information on Internet;
- explain cyber forensic methods;
- understand various kinds of threats over Internet;
- understand how to secure business transactions over Internet; and
- explain about various types of security measures and enforcement.

11.1 INTRODUCTION

The whole world is facing the problem of how to fight cybercrime and how to effectively promote security to the citizens and organizations. If we go into a backdrop, we will quickly understand that Cybercrime, also called computer crime are basically the use of a computer as an appliance to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy etc.

To deal with these emerging crimes a coordinated global response to the problem is required. Cybercrime is growing in a big way and current technical models to deal with cyber offense are disorganized in stemming the boost in cybercrime. This serves to indicate that further preventive strategies are required in order to reduce cybercrime. This, unit throws a light on various aspects related to cybercrimes in its further sections and various security measures one can take to come out from the havoc as whole world is now moving from brick-&-mortar system to Click-&-mortar system.

11.2 CYBER SECURITY MEASURES

As we know that the Internet has changed business, education, government, healthcare, and even the ways in which we interact with our loved ones—it has become one of the key drivers of social evolution. It is one of the main reasons that malicious links, trojans and viruses are entering through internet. The data, breaches are becoming more frequent, and unsuspecting users are more dependent than ever in advance. When one click can cost thousands, and even millions, users need actionable to do’s that can facilitate them to stay attentive and safe online. Cybercrimes, unlike traditional crimes which are committed in one geographic location, are committed online and it is often not clearly linked to any geographic location which means it is not jurisdiction centric. Computer security, cyber security or information technology security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

11.2.1 Role of Cyber Security Analysts

The everyday work of an information security or cyber security analyst will fluctuate, based on where they work, but in general, cyber security analysts’ jobs lead to: Monitoring security access. Security analysts will assess passwords, badges, log-ins, and more as they work to keep a site or system safe. Cyber security analysts (also called information security analysts) map and carry out security measures to take care of a company's computer networks and systems. They keep continuous tabs on threats and supervise their organization's networks for any breaches in security. On the other hands the responsibilities is much wider some the major roles of security analyst are:

- Set and implement user access controls and distinctiveness and access management systems.
- Monitor network and application performance to categorize and lopsided activity.

- Carry out regular audits to ensure security practices are compliant.

11.2.2 Essential Cyber Security Measures

Various essential cyber security measures are provided below:

- Use strong passwords
- Strong passwords are vital to good online security
- Control access
- Put up a firewall
- Use security software
- Update programs and systems regularly
- Monitor for intrusion
- Raise awareness

In further sections the unit has discussed various robust cyber security measures in detail.

11.2.3 Precautionary Cyber-Security Measures Enterprise Takes

As we know that every business is moving online. To achieve the cyber-security basics certain things, need to be taken care as discussed below:

- **A Unified Threat Management (UTM) System:** There must be a combination of security appliances which acts as the gateway to the internet.
- **A Spam Filter:** A spam filter is a program that is used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox. Like other types of filtering programs, a spam filter looks for definite criterion on which it bases judgments. On the other hands it stops potentially malicious files from entering The network via email.
- **Antivirus/anti-malware software**: Antivirus software was originally developed to detect and remove computer viruses, hence the name. Antivirus software, or anti-virus software (abbreviated to AV software), also known as anti-malware, is a computer program used to prevent, detect, and remove malware. These are applications which protect servers, laptops and other devices from malware.
- **Patch Management System:** It manages the installation of software updates to close security holes.
- **2-Factor Authentication:** This gives a second level of authentication, preventing unauthorized sign-ins.
- **Device Encryption:** This makes any data stored on the machine useless to criminals and keeps data secret.
- **Routine Data Backup:** This should keep a copy of business data at a secure off-site location in case the original is lost.
- **Content Filtering:** This prevents access to hazardous or prohibited websites which reduces the risk of infection.
- **Disaster Recovery Plan:** This sets out how one will recover from a spontaneous occurrence such as fire or cyber-attack.

11.3 IOT AND ITS IMPACT

IoT is an acronym used for Internet of Things; it is basically a network of several devices which are attached with miscellaneous software, electronics, and network connectivity of distinct orientations, aimed at exchanging and compiling of any kind of information. The amount of data that IoT devices can create is very gigantic. The vast diffusion of connected devices in the IoT has created enormous demand for robust security in response to the growing demand of millions or perhaps billions of connected devices and services worldwide.

Since the devices which are using IoT technology are supposed to be connected through Internet all the time, it puts up the questions on security themselves, their platforms and operating systems, their communications and the systems to which they are connected. To overcome such security challenges, a new set of tools will be required to protect these devices and platforms from both information attacks and physical tempering. Also, there is a need to encrypt the transactions between the devices. Also, there will be an issue of compatibility too because there are many devices with very simple processors and operating systems and are unable to support sophisticated security systems.

We know and depicts from the above paragraph that IoT security is the technology area apprehensive with safeguarding connected devices and networks in the internet of things (IoT). Allowing devices to connect to the internet opens them up to a number of serious vulnerabilities if they are not appropriately protected. IoT security is the act of securing Internet of Things devices and the networks they are connected to. In the business setting, IoT devices include industrial machines, smart energy grids, building automation, plus whatever personal IoT devices employees bring to work.

- Blocking a program behind a firewall or restricting usage to only certain features of the software, saving critical data from leaking. All the devices connected to the network should be updated to the latest software.
- Hardware, software and connectivity will all need to be secure for IoT objects to work effectively. Without security, any connected object, from refrigerators to manufacturing bots, can be hacked. Once hackers gain organizes, they can take over the object's functionality and steal the user's digital data.

11.4 VULNERABLE INFORMATION ON INTERNET

Vulnerability is the inability to defend against a hazard or to act in response when a disaster has crop up. For instance, people who keep going on plains are more vulnerable to floods than people who live higher up. This is what we call economic vulnerability. If we talk in a technological perspective, A computer vulnerability is a cyber-security expression that refers to a deficiency in a system that can leave it open to attack. This vulnerability could also refer to any type of weakness occur in a computer itself, in a set of procedures, or in anything that allows information security to be exposed to a threat.

Fig 11.1: Various vulnerable terms in cyber world

Now, almost every business has a data driven processes. If a machine or a computer starts running business transactions, the business person might not be proficient to sell to the customers or place orders with the suppliers when the machine is not in order. It may also take place sometimes that a trespasser tries to penetrate the computer system and steals or destroys business data, confidential payment details of the customers. In such a scenario, any business might never be able to operate. Accordingly, for success of any business, data security should be on a top precedence. There should be policies, procedures, and technical measures in the business organizations to prevent unauthorized access, alteration, theft, or any kind of physical damage to information systems.

11.4.1 Vulnerabilities of Systems

When a large volume of digital information is stored, it is vulnerable to many other types of threats. Information systems can be interconnected at multiple locations through computer networks. And hence, the intruder's attack or an unauthorized access can anytime happen at any access point in the computer network, which can destroy the whole network.

In the same manner, the multi-tier client/ server computing environment is also vulnerable at each layer. It is always possible for an unauthorized person to steal or alter valuable data of the organization over networks, during data transmission. Intruders may also use denial of-service attacks or malicious software to interrupt the operations.

11.4.2 Internet Vulnerabilities

Instead of computer networks, the systems connected through Internet, are more vulnerable because they are open to anyone in the whole world. The Internet is so big that it can have an incredibly widespread effect when abuses happen. When the Internet is used in our corporate network, we are much more vulnerable to external operations in the information networks of the enterprise. Computer systems that are permanently linked to the internet are more vulnerable to outside persons' penetration because they can quickly register with fixed IP addresses.

Fig-11.2 (a): Vulnerability though Internet

Fig-11.2 (b): Fixing Vulnerability though Internet

A fixed IP address provides hackers with a fixed target. If the telephone service is not connected to a secure personal internet network, the internet infrastructure that is switched is most vulnerable. The majority of public Internet Voice over IP (VoIP) traffic is not encrypted so that anyone who has a network can hear a debate. Conversations can be stopped by hackers, or voice services shut down, by flooding VoIP supportive servers. The vulnerability of the mail, instant messaging (IM) and peer to peer file-sharing services was also increased. It is possible for workers to use emails for transmitting valuable company secrets, financial data or sensitive information to unauthorized recipients, as malicious software springs boards or unauthorized access to corporate systems internally. Popular IM applications do not use a secure word layer to allow external users to intercept and read it when transmitting the public Internet. In certain cases, instant messaging via the Internet may be used as the back door to a secure network. Sharing in peer-to-peer files (P2P) may also spread malicious software or expose personal or corporate information.

11.4.3 Wireless Security Challenges

Wireless networking provides many advantages, but it is also coupled with various security threats. Implementation of technological solutions to wireless security threats and vulnerabilities, wireless security is a primary necessity of an organization. It is not safe to use a wireless network at public place like, an airport, library, shopping mall etc. In fact, the wireless network at home is not safe because anytime the radio frequency bands can be scanned easily. Hence, LANs, Bluetooth, Wi-Fi networks etc. all are vulnerable to hacking easily. The wireless networks have four basic components:

- The transmission of data using radio frequencies
- Access points that provide a connection to the organizational network
- Devices e.g. - laptops, PDAs, etc.
- Users.

These components may become the source for attack due to which the organisation has to compromise the data. Furthermore, in a Wi-Fi network, intruders can easily collect the identity Service Set Identifiers (SSIDs), which mark access points, transmit a number of times and thus. Wi-Fi networks usually do not have fundamental safeguards, which allow unauthorized users to access the network in the surrounding buildings or outside the site. An attacker that has an access point with the correct SSID may access other network resources. Also, intruders can use the information they gather to set up unauthorized access points for the radio Network Interface Controller (NIC) of a user in a different radio channel near the website. Hackers using the rogue access point will collect unsuspecting users' login credentials once this association is formed.

11.4.4 MaliciousS oftware

These are also known as malware which include a number of threats, eg- computer viruses, worms, and Trojan horses.

- **Computer virus:** A computer virus is a software program that attaches itself to other software programs or data files in order to be executed. It does not seek any permission of the user before execution of the program.

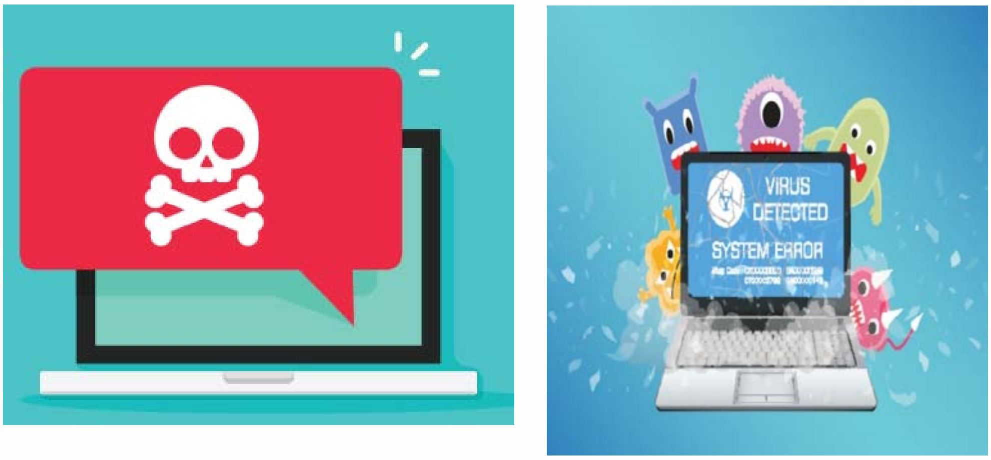


Fig 11.3: Computer Virus

Virus may be highly destructive which may destroy data of the organization completely, block computer memory, reformat a computer's hard drive or cause the programs to run improperly. Viruses may spread from machine to machine, for example, through an e-mail attachment or an infected file.

- **Worms:** Worms are independent computer programs which use a computer network to copy themselves from one computer to other computers. These can operate on their own without any human intervention and there is no need to attach it to any computer program files.

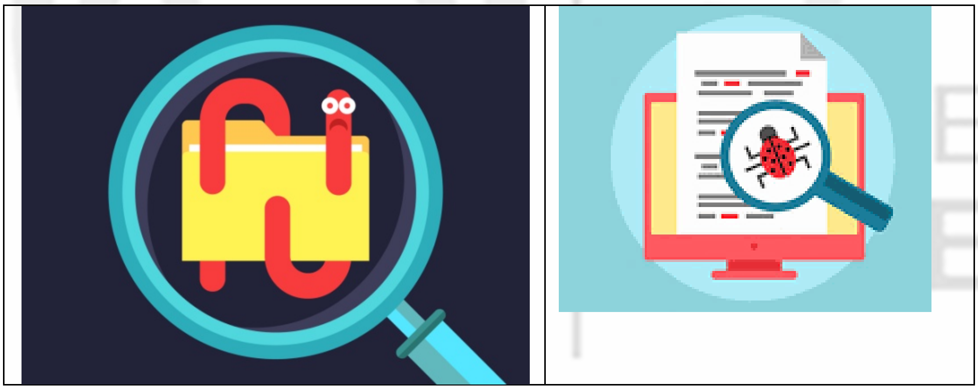


Fig 11.4: Computer Worms

Worms spread much more promptly than computer viruses. Worms are very harmful for data and programs. These may choke the whole computer network.

- **Trojan horse:** Another malware is Trojan Horse which attacks on the data silently. The Trojan horse is not a virus itself, but it gives a path to viruses to enter into the systems. For example, ZeuS (Zot) Trojan which infected more than 3.6 million computers in past years and still poses a threat. This software helped the unauthorized person to steal the bank login credentials of the customers secretly by catching their passcode keystrokes as they used in their computers. Zeus is spread through phishing.

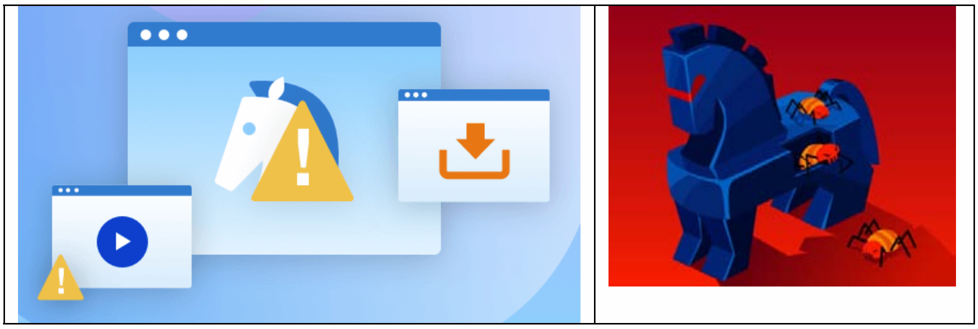


Fig 11.5: Trojan Horse

- **SQL injection attacks:** SQL injection attacks take benefit of weak points of web application software which are not robust in terms of security check or which do not have sufficient code written into them for data security. Such attacks introduce malicious programs into system and networks of the organisations.

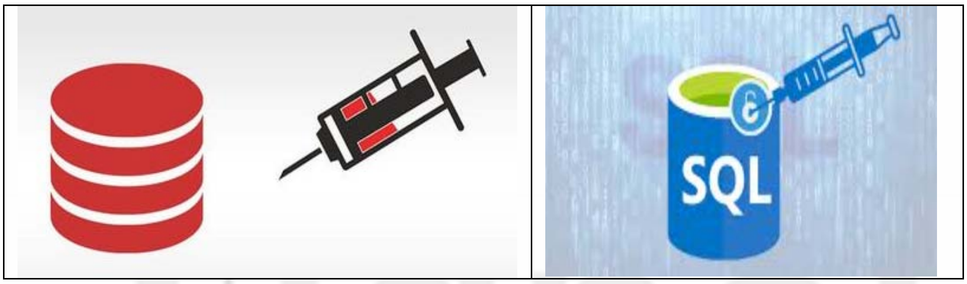


Fig 11.6: SQL Injection

- **Ransomware:** There is a malware known as ransomware which blocks access to files and displays lots of pop-up messages and extracts money from users by taking control of their systems. For example, the ransomware ware called 'WannaCry' that attacked computers in more than 150 countries in the past years. It encrypted the files of the system and then asked users to pay lots of money to recover access. Ransomware may enter to your system by downloading unauthorized email's attachments, or downloading a file from an unsafe link. Few malwares are spywares. Spywares install themselves secretly systems to watch activities of the users. Multiple types of spyware exist which try to breach the privacy of the users.

Fig 11.7: Ransomware

- **Keyloggers:** Another one is Keylogger which records every keystroke made on a computer or mobile phone to steal serial numbers or another codes of software for attacking on the data of the user, to gain access to email accounts or passwords or to fetch credit/debit card details or other financial data. Few spywares reset web browser home pages, redirect search requests or slow performance by taking up too much computer resources.

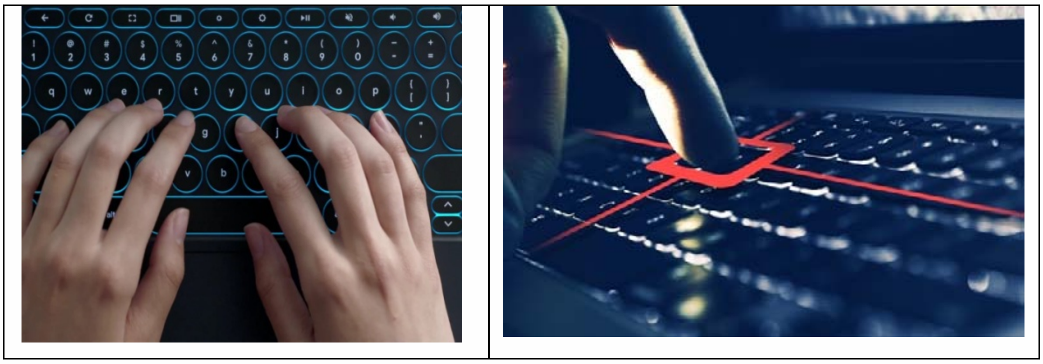


Fig 11.8: Keylogger

11.4.5 Hackers and Computer Crime

A hacker is an intelligent coder whose aim is to achieve access to a computer system of another user. They can request malicious files without any human intervention, destroy useful data, transmit data, and install a hidden program running in the background to monitor user actions. They are experts and know methods of gaining unauthorized access by finding weaknesses in the security protections employed by Web sites and computer systems. The purpose of hacking a system is to steal data or secrete information, to damage system, defacement, destruction of a Web site or corporate information system etc. The mobile platform that most hackers use is Android, world's leading mobile operating systems. Viruses on mobile devices pose grave threats to company computing as many cellular devices are now related to corporate information systems. Social networking sites such as Facebook, Blog sites etc. have also become the source of malware or spyware. Members are more likely to trust messages they receive from friends, even if this communication is not authentic. Various types of computer crimes by hackers are discussed below:

- **Spoofing and Sniffing:** In order to gain access to sensitive information of the users, hackers generally pretend to be someone known to the users. This is called spoofing. Sometime, hacker also shares a web link with the users which are entirely different from the original website, to befool the users. In this manner, the hacker may collect and process orders, effectively stealing business as well as sensitive customer information from the original site.

  Sniffing is the mechanism by which data packets move through a network of computers via sniffers can be monitored and captured. Network administrators use Packet Sniffers for monitoring data traffic through their network. These are called analyzers of network protocols. Sniffers can identify possible network vulnerabilities or illegal activities on networks, but can be dangerous and very difficult to detect if used negatively. Sniffers allow the hackers, including emails, company files and confidential reports, to steal sensitive information from any part of the network.

- **Denial-of-Service Attacks:** When a hacker does such an activity due to which the server of an organization starts receiving huge requests for some service, the server stops responding to the genuine requests also due to congestion or crash of the network. This is called distributed denial-of-service (DDoS) attack. Although DoS attacks do not destroy information or access restricted areas of a company's information systems, they often cause a Web site to shut down, making it impossible for genuine users to access the site. These attacks are very dangerous for e-commerce sites as these make the site shut down because it is inaccessible to customers.

  DDoS attacks also use tens of thousands of "zombie" PCs, which have not become a botnet, infected with malicious software. These botnets are created by hackers who infect other people's computers with bot malware that opens a back door to send orders from an intruder. A slave or zombie is transformed into the infected machine that serves a master computer from another human. Hackers may use the botnet's accumulated resources to conduct attacks on DDoS, phishing campaigns or unselected "spam" e-mail until they infect enough computers

11.4.6 Cyber Crime

Any criminal activity or data theft which is done by using Internet is called cybercrime. Various types of cyber crimes are explained in detail below:

- **Identity Theft:** As more and more people have started using Internet and doing online transactions, the problem of identity theft is increasing day by day. It is one of the cyber crimes in which personal or financial information is acquired by some unauthorized person over internet to harm the user. The information may be used to steal money from the bank of the account holder or to purchase lots of things, merchandise, or services by using credit card in the name of the victim or to provide the thief with false credentials.

  Identify fraud on the internet that has been a big goal of website hackers with credit card files. Often, different types of e-commerce sites are one of the origins of a crime in which cyber criminals collect personal information from their users in order to render consumer fraud.

- **Phishing:** One increasingly popular tactic for identity theft is called Phishing which involves setting up fake Web sites that looks like those of real websites to ask users for their personal or financial data. Sometimes e mails are also sent to the victims along with links of fake websites which resembles the home page of their bank's website. In a more targeted form of phishing called spear phishing, which befools the users through text messages or social media messages and appear to come from a trusted source.

  Phishing can be classified in two ways, known as evil twins and pharming which are even more difficult to identify.

i. **Evil twins:** These are wireless networks that pretend to offer trustworthy Wi-Fi connections to the Internet, such as those in airports, hotels or shopping malls. The fake network looks same to an authentic public network. Passwords or credit card numbers of innocent users are captured by cyber criminals as soon as they log on to the network.

ii. **Pharming:** Pharming redirects users to a fake web page, even after typing the right URL of the website. This is also known as "The phishing without a lure". The cybercrime of phishing attracts many penal provisions of the Information Technology Act, 2000.

- **Pay-Per-Click Fraud:** For all kinds of sponsored search results displayed by a search engine, the advertiser pays fee for each click it receives, with a result of increased potential buyers to the products. Click fraud occurs when an individual or computer program deceitfully clicks on an online ad without any intention of learning more about the products displayed in the ad to purchase it. Click fraud has become a serious problem at Google and other Web sites that feature pay-per-click online advertising. Because of the competition between companies, few companies employ third parties to click on advertising from the competitor to exacerbate their performance by - marketing expenditure. This fraud can also be done with clicking software programmes, for which botnets commonly are used. Search engines like Google are attempting to track this fraud but are reluctant to publicize their efforts.

11.4.7 Global Threats: Cyber Terrorism and Cyber warfare

All the cybercrimes that have been discussed so far are borderless as the medium of travel is Internet. It can travel everywhere in every country and harm anywhere in the world. China, the United States, South Korea, Russia, and Taiwan are currently the sources of most of the world's malware In fact, countries are trying to damage the economies of their competitors, spying them by using such cyber activities. The "Cyber warfare" is a state-sponsored activity aimed at smashing, defying and inflicting harm and destruction on a state or nation through intrusion on their computers or networks.

Generally speaking, cyber warfare attacks are becoming more common, sophisticated and potentially destructive. In the course of years, hackers have robbed plans for missile tracking systems, satellite navigation equipment, defense drones and advanced jet fighters. Since their key financial, health, government and industrial institutions depend on Internet to conduct their day-to-day operations, cyber warfare poses a severe threat to modern society infrastructure. It also includes defending cyber warfare against such attacks. The Interactive Organization Session explains some recent cyber war attacks and their increasing sophistication and gravity.

11.5 CYBER FORENSIC

Cyber forensic is a branch of digital science in computers and digital storage media which has facts. In order to respond to legal action, data protection and control management have become extremely essential. Today, a lot of the evidence is available in digital form for inventory fraud, misappropriation, theft of business secret data, cybercrime and several civil cases. In addition to facts from printed and type-written pages, legal cases today depend on evidence portrayed as digital data stored on mobile storage devices, CDs and hard disc machines, and on Internet email, instant messages, and e-commerce. The most popular form of electronic proof nowadays is e-mail.

In a legal action, a firm has to respond to a discovery request for access to information that may be used as evidence, and the company is required by law to produce the required data. The cost of responding to a discovery request can be huge if the company has trouble displaying the required data or the data have been corrupted or destroyed. Courts now impose severe financial and even criminal penalties for improper destruction of electronic documents.

A special policy for the preservation of electronic documentation ensures that files, e-mails and other records are organised well, accessible and neither too long nor too soon is kept. It also represents an understanding of how digital forensics can be maintained. In computer forensics, the scientific data processing, study, authentication, preservation and analysis is used in a way that the information is used as evidence in court of law and that is preserved or recovered from computer storage media. The following issues are addressed:

- Recover computer data while ensuring the credibility of proof
- Secure electronic data storage and handling
- Finding vast volumes of electronic data for essential details
- Submitting to a court of law the details

Electronic proof can be found in the form of data on computer storage media not apparent to the regular person. An example is a file that has been deleted on the PC hard drive. Data can be removed by a user on computer storage media by different techniques. Software forensic experts attempt to retrieve confidential data to show. Software forensics awareness should be integrated into the contingency planning phase of a business. The CIO, security professionals, information technology personnel and corporate counsel must work together to implement a strategy which, if legal requirements occur, can be enforced.

Check Your Progress A:

1) Distinguish between spoofing and sniffing.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

2) What are the various global threats of cyber terrorism?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

3) How does pay-per-click fraud occur?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

4) How do hackers execute computer crimes?

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

11.6 SECURING THE BUSINESS ON INTERNET

With the constant stream of new technologies, companies are rapidly changing their IT environments to keep a step ahead of their competitors. However, implementing the e-business applications may be impossible without a coherent, consistent approach to e-business security. Failure to protect information assets from external and internal intruders can lead to embarrassing public exposure, loss of customer confidence and financial loss. A company's decision to protect itself is not just a technology decision. It is a business decision.

Ensuring the security of corporate assets is a continuous and dynamic process, rather than an item on a checklist that can be forgotten once it is set up. The solutions' openness and extensibility give to a global communications company the flexibility to leverage existing technologies and adopt new ones as its e-businesses evolve.

- **Technologies and Tools for Protecting Information Resources:** Companies have a variety of information resources security technologies. These include instruments to manage user identities, prevent unauthorized access to systems and data, ensure the available framework and guarantee the quality of software.
- **Identity Management and Authentication:** Medium-sized and large businesses have several separate IT infrastructures and processes, each with own user community. Identity software automates the process of monitoring the device rights of all these users, granting each user a unique digital identity to access each system. It also provides tools for user authentication, user identity security and device access control.

To gain access to a system, authentication is must for a user. Authentication means the ability to know that the right person is accessing which is established by using username and password known only to the authorized user. But user passwords are also lacking, they are shared and weak passwords are chosen. Excessively difficult login schemes hinder employee efficiency. Users typically prefer easy passwords that enable complex passwords to be transferred, and few users also write or hold their passwords near their workstations easily available. Social engineering tricks sent over a network can also rob passwords.

Any of these issues are solved by modern authentication methods such as keys, intelligent cards and biometric authentication. A token is a physical instrument, similar to an ID card designed to prove a single user's identity. Tokens are tiny devices that generally fit on key rings and often change pass codes.

11.7 SECURING NETWORK TRANSACTION

Various ways of securing networks transactions are discussed below:

- **Securing wireless networks:** The Wired Equivalent Privacy (WEP), initial security standard developed for Wi-Fi, is not very successful, because the encryption key is comparatively easy to crack. However, if users remember to allow it, WEP provides some margin of protection. The use of Virtual Private Network (VPN) technology in access to internal corporate data will further enhance Wi-Fi security. It also operates an encrypted authentication scheme with a central authentication server to ensure that the network is accessed only with the approved users.
- **Encryption and public key infrastructure:** Encryption is one of the most common methods to protect digital information stored or shared by

the organizations over the Internet. It is the process of transforming plain text or data into encrypted data, called cipher text so that an unauthorized person cannot read it. It can be read only by receiver and sender. A secret numerical code, called an encryption key is used to transforms plain data into cipher text. The message must be decrypted by the receiver. The receiver is supposed to decrypt the data by using another key or the same key. There various methods for encrypting network traffic on the Web as discussed:

- **Secure Sockets Layer (SSL):** SSL is a protocol used for encrypting data flowing over the Internet. Along with Transport Layer Security (TLS) enable client and server computers to manage encryption and decryption activities as they communicate with each other during a secure Web session. SSL and TLS are designed to establish a secure connection between two computers.

- **Secure Hypertext Transfer Protocol (S-HTTP)**: It is another protocol used for encrypting data flowing over the Internet, but it is limited to individual messages. Internet client browser software and servers generate the secure session. The client and the server discuss what key and what level of security is required to use. Once a secure session is established between the client and the server, all messages in that session are encrypted.

- **Symmetric key encryption**: In symmetric key encryption, the sender and receiver create a secure Internet session by creating a single encryption key and sending it to the receiver, as a result, both the sender and receiver share the same key. The strength of the encryption key is measured by its bit length. Today, a typical key will be 128 bits long (a string of 128 binary digits).There is a drawback with symmetric encryption key that the key itself must be shared among the senders and receivers, which exposes the key to outsiders who might just be able to capture and decrypt the key.

- **Public key encryption**: This is more secure form of encryption which uses two keys-

    - Public-owned by sender, encrypts the messages

    - Private-owned by the receiver, decrypts the messages

  To send and receive messages, communicators first create separate pairs of private and public keys. The public key is kept in a directory and the private key must be kept secret. The sender encrypts a message with the recipient's public key. On receiving the message, the recipient uses his or her private key to decrypt it.

- **Digital certificates:** These are data files for identifying online transaction users and electronic properties. A digital system of certificates uses a trustworthy third party called a Certificate Authority (CA) to verify the identity of a user. Many CAs, including Symantec, GoDaddy and Comodo, are available in the USA and worldwide. When Certifying Authority verifies a digital certificate of the user offline, a digital encrypted certificate containing owner identity information and a copy of the public key of the owner is produced from the CA server.

The certificate ensures that the appointed owner has the public key. The CA provides its own public key on the web in print. The receiver of an encrypted message uses the public key of the CA to decipher and validate the digital certificate attached to the message and then obtain public key information and identity details found in the certificate. The recipient may submit an encrypted response by using this information. A credit card consumer and a merchant may verify their digital certificates by using digital signatures before exchanging data from an accepted and trusted individual. In electronic commerce, Public Key Infrastructure (PKI) is now commonly used in use of public key cryptography that operates with a CA.

- **Securing transaction with Blockchain:** It is an alternative approach for securing transactions and establishing trust among multiple parties. A Blockchain is a chain of multiple blocks that contain records of transactions. Each block is connected to all the blocks before and after it and block chains are continually updated and kept in sync. This makes it difficult to tamper with a single record because one would have to change the block containing that record as well as those linked to it to avoid detection.

  Once recorded, a Blockchain transaction cannot be changed. The records in Blockchain are secured through cryptography and all transactions are encrypted. Blockchain network participants have their own private keys that are assigned to the transactions they create and act as a personal digital signature. If a record is altered, the signature becomes invalid and the Blockchain network will know immediately that something is inappropriate. Because block chains are not kept at a central location, they don't have a single point of failure and cannot be changed from a single computer. Blockchain is suitable for environments with high security requirements and mutually unknown actors.

- **Fault-tolerant computer systems:** Fault – tolerant computer system have redundant hardware, software, and power supply components that create an environment that provides continuous, uninterrupted service. Fault-tolerant computers use special software routines or self-checking logic built into their circuitry to detect hardware failures and automatically switch to a backup device. These are special systems such that different parts from these computers can be removed and repaired without any disturbance to the computer system.

- **High-availability computing environments:** High availability computing environments are generally used for e-commerce applications which have very less requirement for heavy e-commerce processing where the organisations depend on digital networks for their internal operations. There is a need of backup servers, distribution of processing across multiple servers, high-capacity storage, and good disaster recovery and business continuity plans for a good execution of High-availability computing. Also, it needs extremely robust computing platforms with scalable processing power, storage, and bandwidth to function properly. Both fault tolerance and high-availability computing are used to minimize downtime. Downtime is the period of time in which a system is not able to perform. Comparatively, high-availability computing helps firms recover quickly from a system crash than fault tolerance systems.

- **Deep Packet Inspection (DPI):** It can sometimes be noticed that the university network on the campus is very sluggish. This may happen if anyone uses the network to download music or see YouTube, or another hard-to-download video, as the bandwidth of the application is heavily used and the campus network has slowed down, slowing down the download speed on other users' devices. Deep packet inspection (DPI) technology solved this problem. DPI examines data files and sorts out low-priority online material while assigning higher priority to business-critical files. Based on the priorities established by a network's operators, it decides whether a specific data packet can continue to its destination or should be blocked or delayed while more important traffic proceeds.

- **Security outsourcing:** There are various organisations which are unable to acquire the security measures and resources to provide a secure high-availability computing environment to their workforce. Generally, it happens with mid-level or small-scale industries. Such organisations may outsource many security functions to manage their security services from Managed Security Service Providers (MSSPs)for monitoring network activities and perform vulnerability testing and intrusion detection. Secure Works, BT Managed Security Solutions Group, IBM, Verizone, AT&T and Symantec are leading providers of MSSP services.

- **Security issues for cloud computing and mobile digital platform:** Cloud computing and the mobile digital platforms have become the backbone of data collection, analytics and then predictions. These technologies potential to deliver powerful benefits. But at the same time, these technologies have given a few challenges to system security and reliability. We now describe some of these challenges and how they should be addressed.

1 **Security in the cloud:** Web-based firms which are very sophisticated and use cloud service may experience security collapses. The organization which owns the sensitive data has accountability and responsibility for protection. Understanding how the cloud computing provider organizes its services and manages the data is a little complex.

Cloud computing services are made distributed. Cloud systems reside in large remote data centers and server farms providing multi-company clients with enterprise and data management. Cloud providers also assign work to data centers around the world in order to save resources and keep costs down. No one knows exactly where the data is located while using the cloud.

The downside is, however, that it is difficult to monitor illegal activity due to the distributed existence of cloud computing. Almost all cloud providers use encryption to protect data they control when transmitting the data, for example, with the Secure Sockets Layer (SSL). But it is important to ensure that the data is encrypted if data is stored on devices that also store data by other companies.

Companies expect their systems to be running day and night continuously, but cloud providers haven't always been able to provide this kind of service. On several occasions over the past few years, the cloud services of Amazon.com and Salesforce.com experienced outages that interrupted business operations for millions of users.

Cloud users must ensure that they are secured at a level that satisfies their business requirements, regardless of where their data is saved. The cloud provider can enter and process data under the data security laws of certain jurisdictions in some jurisdictions. Cloud customers should find out how their company data are isolated from the other companies by a cloud provider and obtain evidence of a sound encryption process. It is also important to know how the cloud provider will respond in the event of a catastrophe, whether the provider will fully recover your data and how long. Users in the cloud must also inquire if cloud services will be subject to external audits and security approvals. Such reviews can be written into the SLA agreement before a cloud provider is signed.

2 **Securing mobile platforms:** If mobile devices perform many of the computer functions, they have to be protected against malware, theft, accidental loss, unauthorized entry and hacking, such as desktops and laptops. Special protection is required for mobile devices which access company systems and data. Companies should ensure that their corporate security strategy encompasses mobile devices and specifics of how to support, secure and use mobile devices. Mobile device management tools are necessary to approve all devices in use, keep correct inventory data on all mobile devices, users and apps, maintain updates of applications and lock or remove devices lost or stolen so that they cannot be jeopardized. Corporate guidelines for licensed mobile platforms and software applications as well as required software and remote access procedures of company systems should be established by businesses.

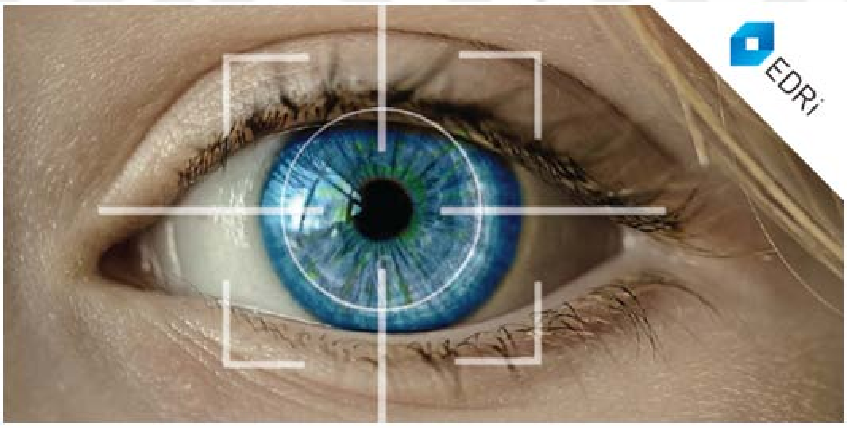
Companies can, wherever necessary, encrypt contact. The password feature found on each Smartphone should be needed for all mobile device users. Some businesses demand that workers only use smartphones from the company. Since BlackBerry devices run on their own safe systems, they are considered safest. But more and more businesses are empowering employees to make employees more accessible and efficient on their own devices, including iPhones and Android phones. For the isolation of corporate data stored in personal mobile devices from their personal information, protecting software products like the Good Technology tools are now available.

11.8 SECURITY MEASURES AND ENFORCEMENT

Taking into consideration information is the most precious asset of an organization; information security is one of the most significant areas for every business and individual. Looking at the big picture, approximately 86% of all websites had a serious vulnerability which is an observation omni presents in past and in present too.

11.8.1 Biometric Security Measures

In order to grant or deny entry, biometric authentication uses devices that read and interpret individual human traits, such as fingerprints, irises and voices. Biometric authentication is based on a physical or behavioral characteristic measurement, which is specific for each person. It compares the unique characteristics of a person, such as fingerprints, face or retinal images, to a stored profile, to see if any variations exist between them and the stored profile access is given when the two profiles match. Finger printing and face recognition technologies have only recently begun to be used in several laptops with fingerprint authentication systems, as well as many models with built-in webcams and face recognition apps, and for security applications. Financial service firms such as Vanguard and Fidelity have implemented voice authentication systems for their clients.



***Source:** edri.org

Fig 11.9: Biometric

11.8.2 Non- Biometric Security Measures

Connecting to the Internet will be very risky without protection against malware and intruders. The essential business tools have been firewalls, intrusion detection systems and antivirus software. These are explained below in detail:

- **Firewalls:** Unlicensed users cannot access private networks with firewalls. A firewall is a hardware-to-software combination that controls traffic input and output. It is typically positioned between private internal networks and distrustful external networks such as the Internet, though a portion of the company's network can also be shielded by firewalls from the remainder of the network.

The firewall functions as a porter that checks the credentials of each user before a network access is provided. It defines input traffic names, IP addresses, applications and other features. This information is managed by the network administrator against the access rules that the system has programmed. Firewall prohibits unwanted contact into the network and out of it and lies on a specially designated device in large organizations which is isolated from the rest of the network, so that no incoming request has direct access to private network resources. There are many technologies for firewall screening including static packet filtering, state-of-the-art inspection, network address translation and proxy filtering. They are also used as a firewall security mix.

The packet filter analyses the selected fields of the data packet header, which scans individual packets isolated between the trusted network and the Internet. This filtering technology can skip several forms of attacks. Full inspection offers greater security by assessing whether shipments are part of ongoing conversation between sender and recipient. It develops tables for tracking information in several shipments. Packs are allowed or rejected for the purpose of belonging to the permitted discussion or attempting to have a legitimate relationship. When static packet filtering and inspections are carried out, Network Address Translation (NAT) may provide additional layer security. NAT masks the IP addresses of the internal host computer of the company in order to avoid revealing sniffer programmes outside the firewall and use that information to infiltrate internal systems.

Filtering the application proxy checks the packet application content. A proxy server pauses, inspects, and transfers a proxy to the other side of the firewall data packets originating outside of the company. If a user outside the company wishes to connect with the user inside the company, the external user can speak to the proxy application first and the proxy application contacts the internal device of the company. Likewise, in the company a computer user moves through the proxy to converse with outside machines. To build a successful firewall, an administrator must maintain detailed internal rules that define the authorised or denied individuals, applications, or addresses. Firewalls can disrupt the penetration of the network by externals, but they cannot entirely prevent them from doing so.

- **Intrusion Detection Systems:** Commercial protection vendors also offer software and services for detecting intrusions against suspicious network traffic and for attempting to access files and databases in addition to the firewalls. Full-time monitoring tools for detect and deter intruders are included in intrusion detection systems at the most vulnerable points or "hot spots" of the business networks. If a suspicious or anomalous incident happens, the device may trigger an alert. Scanning software searches for trends that indicate known methods of attacking machine, such as bad passwords and checks if essential files were deleted or changed. Computer monitoring examines incidents when security attacks are detected. If an unwanted traffic is received, the intrusion detection instrument may also be modified to shut down a specifically sensitive part of the network.

- **Antivirus and Antispyware Software:** The defense protection plans need to protect all devices, both for individuals and companies, against malware. Malware such as computer viruses, computer worms, tropical horses, spyware and adware is stopped and detected by antiviral. Most antivirus software is effective only when it is written against already known malware. To continue to be effective, the antivirus software must be continuously updated.

- **Unified Threat Management Systems (UTM):** Since a huge cost is applied to avail such security services and it is not easy to access such facilities by small and medium business organisations, security products with reduced costs and improved manageability are introduced in the market which have combined security methods into a single appliance and include firewalls, virtual private networks, intrusion detection systems, and Web content filtering and anti-spam software. These comprehensive security management products are called unified threat management (UTM) systems. Although initially aimed at small and medium-sized businesses, UTM products are available for all sizes of networks. Major players of UTM in the market are Crossbeam, Fortinent, and Check Point, and networking vendors such as Cisco Systems and Juniper Networks provide some UTM capabilities in their equipment.

11.8.3 Cyber-Physical Security System

Cyber-Physical Security Systems (CPSS) equipment can play an important role in enhancing the security of the organisations. However, they must not be deployed in isolation. Cyber Physical Security System technologies are only as effective as the overall security plans, processes and procedures they support. CPSS should be implemented as part of a larger, coordinated safety strategy of the organization that takes into account the impact on the networks, security personnel and employees. There are various types of cyber physical security systems:

- **Surveillance:** Video cameras can deter crime, identify campus visitors, and provide real-time information during an active threat situation. Passive Monitoring refers to recorded data that is analyzed at a later time, usually as part of an event investigation. Active Monitoring involves personnel watching a live video feed. Some districts have agreements with law enforcement to provide real-time video feed access during a security incident.

- **Communications equipment and platforms:** Wired and wireless communication technologies, such as intercom systems, local alarm enunciators, phone systems, and two-way radios are used by school officials and emergency personnel during emergencies. Enhanced 911 (E911) and other location-based communications identify the location from which calls or messages are sent. Attendance and Check-In Apps can be used to track student presence on campus and allow school staff to account for students during an emergency incident.

- **Sensors and alarms:** sensors and alarms can be used to notify personnel on and off campus that an emergency is taking place. Mapping and verification solutions can help personnel the exact location of the emergency and provide audio and/or video input officials determine the nature of the threat.
- **Duress alarms (panic buttons):** These are wired or wireless devices that can be used to notify school officials and emergency personnel about an emergency. Some devices also transmit the sender's identity in addition to location. Door and Window Sensors can send alerts or trigger alarms when doors and windows have been breached. Gunshot Detectors can identify the location and caliber of a gunshot. They can be integrated with comprehensive security systems which can alert authorities, point cameras at the impacted area, and lock doors.
- **Robots:** Robots integrate a number of security features, including facial and object recognition and streaming video, can serve as the eyes and ears for emergency responders.
- **Lighting:** It should be considered to provide safe passage in an emergency and improve overall campus security. In addition to highlighting emergency exit routes, lighting can be used for communications, such as allowing law enforcement to identify locations that have been cleared during a security incident.
- **Fogging and pepper spray systems:** It creates a smokescreen or deploy chemical aversive and are often put in vestibules. However, these run the risk of hampering responder operations and can be compromised or misused.

11.8.4 Access Control

Access Control is the selective restriction of access to places or other resources. Access control can be accomplished by using a human resource (such as a security guard), mechanical means (such as locks and gates) or a technological solution (such as swiping an ID card). Examples of access control solutions include:

- **Locks, Gates, and Vestibules:** Experts recommend that university campuses be closed during the worked day with only one entrance point and software enabled cameras are there. Office personnel may clear outsiders to enter through a secure vestibule, which may be built of bullet-proof glass or enhanced with a shatter-proofing film with a software enabled camera are equipped.
- **Metal Detectors**: Some university use metal detectors to prevent students, staff, or visitors from bringing guns or other weapons onto the university campus.

- **Door Barriers:** These retrofit security devices turn the door into a barricade to help prevent an attacker from gaining access. Although effective, these products may conflict with local fire codes.

- **Entry Cards:** Entry cards can be used with or without embedded technology. ID cards provide a visual indication of whether or not an individual is authorized to be on a university campus. Some university systems issue ID cards to students, faculty and staff. Visitors may receive guest badges or adhesive stickers. Smart ID cards include a chip that can be used together with a reader to identify student locations during an emergency or allow school staff to unlock doors. Biometric readers such as fingerprint scanners can be used for the same purposes.

- **Access Software**: Specialized software, often used in school offices or other campus entry points, can track visitor histories, print temporary badges, and check databases for registered sex offenders. Facial Recognition software can be used to prevent unapproved individuals from entering a building, match visitors against criminal databases, or help ensure that students board the correct bus. However, this software is in its infancy and concerns have been raised about accuracy and student privacy. Along the same lines, object recognition technology can be used to identify weapons or other prohibited objects. Central Lockdown Capability consists of integrated security systems that can automatically trigger a school lockdown when a panic button is activated, an alarm goes off, or a gunshot is detected.

11.8.5 Ensuring Software Quality

Otherwise, companies can improve system quality and reliability through the use of software measures and rigorous software testing, as well as implement effective security and controls. Software metrics are machine objective evaluations in the form of calculated quantifications. Ongoing use of the metrics helps the IT and end users to collectively assess the system are output and detect issues when they arise. Software metrics are examples of how many transactions can be performed in a given unit of time, how much time online reply time, how many paid checks are shown every hour and how many errors are known per 100 lines of programme code. Metrics must be planned, formalised, objective and regularly used in order to be efficient.

Early, reliable and comprehensive testing can greatly contribute to the consistency of the system. Many regards checking as a way of demonstrating the correctness of their work. We know, in fact, that all the big software has errors and we have to test to detect these errors.

Good testing starts before a software application even uses a systematic analysis — a small group of people who have carefully chosen the expertise required for the particular goals to be tested. When developers begin to write programmes, they may also use coding to rewrite the code. Code must be checked, however, by running a programme. If mistakes are found, a procedure called debugging will find and remove the source.

Check Your Progress B:

1) What are the methods for encrypting network traffic on the Web?

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

2) How do sensors and alarms help in ensuring cyber-physical security?

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

3) What do you understand by security outsourcing?

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

4) What are biometric security measures?

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

11.9 LET US SUM UP

Now, almost every business has a data driven processes. If a machine or a computer starts running business transactions, the business person might not be able to sell to the customers or place orders with the suppliers when the machine is not in order. It may also happen sometimes that an intruder tries to penetrate the computer system and steals or destroys business data, confidential payment details of the customers.

When a large volume of digital information is stored, it is vulnerable to many other types of threats. Information systems can be interconnected at multiple locations through computer Networks. And hence, the intruder's attack or an unauthorized access can anytime happen at any access point in the computer network, which can destroy the whole network. Instead of computer networks, the systems connected through Internet, are more vulnerable because they are open to anyone in the whole world. The Internet is so big that it can have an incredibly widespread effect when abuses happen. Wireless networking provides many advantages, but it is also coupled with various security threats. Implementation of technological solutions to wireless security threats and vulnerabilities, wireless security is a primary necessity of an organization.

A hacker is an intelligent coder whose aim is to achieve access to a computer system of another user. They can request malicious files without any human intervention, destroy useful data, transmit data, and install a hidden program running in the background to monitor user actions. They are experts and know methods of gaining unauthorized access by finding weaknesses in the security protections employed by Web sites and computer systems. The purpose of hacking a system is to steal data or secrete information, to damage system, defacement, destruction of a Web site or corporate information system etc.

Cyber forensic is a branch of digital science in computers and digital storage media which has facts. In order to respond to legal action, data protection and control management have become extremely essential. Today, a lot of the evidence is available in digital form for inventory fraud, misappropriation, theft of business secret data, cyber crime and several civil cases.

Encryption is one of the most common methods to protect digital information stored or shared by the organisations over the Internet. It is the process of transforming plain text or data into encrypted data, called cipher text so that an unauthorized person cannot read it. It can be read only by receiver and sender. A secret numerical code, called an encryption key is used to transforms plain data into cipher text. The message must be decrypted by the receiver.

Biometric authentication uses devices that read and interpret individual human traits, such as fingerprints, irises and voices. Biometric authentication is based on a physical or behavioral characteristic measurement, which is specific for each person. Connecting to the Internet will be very risky without protection against malware and intruders. The essential business tools for non-biometric security measures are have been firewalls, intrusion detection systems and antivirus software etc.

Cyber-Physical Security Systems equipment can play an important role in enhancing the security of the organisations. However, they must not be deployed in isolation. Cyber Physical Security System technologies are only as effective as the overall security plans, processes and procedures they support. CPSS should be implemented as part of a larger, coordinated safety strategy of the organization that takes into account the impact on the networks, security personnel and employees.

Access Control is the selective restriction of access to places or other resources. Access control can be accomplished by using a human resource (such as a security guard), mechanical means (such as locks and gates) or a technological solution (such as swiping an ID card). Examples of access control solutions include locks, gates, and vestibules, metal detectors, door barriers, entry cards, access software etc.

11.10 KEYWORDS

Cyber Forensic: Cyber forensic is a branch of digital science in computers and digital storage media which has facts. Its goal is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Deep Packet Inspection (DPI): DPI examines data files and sorts out low-priority online material while assigning higher priority to business-critical files. Based on the priorities established by a network's operators, it decides whether a specific data packet can continue to its destination or should be blocked or delayed while more important traffic proceeds.

Door Barriers: Door barriers retrofit security devices turn the classroom door into a barricade to help prevent an attacker from gaining access. Although effective, these products may conflict with local fire codes.

Duress Alarms (panic buttons): These are wired or wireless devices that can be used to notify school officials and emergency personnel about an emergency. Some devices also transmit the sender's identity in addition to location. Door and Window Sensors can send alerts or trigger alarms when doors and windows have been breached.

Pay- per- Click Fraud: Click fraud occurs when an individual or computer program deceitfully clicks on an online ad without any intention of learning more about the products displayed in the ad to purchase it. Click fraud has become a serious problem at Google and other Web sites that feature pay-per-click online advertising.

Recovery-Oriented Computing: This involves the design of quick-recovery systems and the implementation of operators' skills and tools to detect and quickly remedy error sources in multi-components systems.

SQL Injection Attacks: SQL injection attacks take benefit of weak points of web application software which are not robust in terms of security check or which do not have sufficient code written into them for data security.

11.11 TERMINAL QUESTIONS

1) What are various types of malicious software's/malwares which induce cyber crimes?

2) What are cyber crimes? State various types of cyber crimes occurring these days.

3) What is cyber forensic?

4) What are the various ways of securing network transactions?

5) What are the various ways of securing the business on internet?

6) What are the various non-biometric security measures?

7) What are the various types of cyber physical security systems?

8) State various access control solutions.

Note	These questions are helpful to understand this unit. Do efforts for writing the answer of these questions but do not send your answer to university. It is only for your practice.