BLOCK 4

Cyber Security and IT Act

BLOCK 4: CYBER SECURITY AND IT ACT

This is the fourth block of the course “E-Commerce”. This block makes the learners familiarize with cyber security, various measures for cyber security, various types of cyber crimes and threats as well as the various highlights of the IT Act. This block is structured to explain the various terminologies related to the cyber word and to understand the various provisions granted under IT Act to aid them when in need. The block on the theme “Cyber Security and Information Act" comprises of three units, the detail of which is mentioned below:

- **Unit-10:** This unit helps the learners to understand the basic terminologies of the cyber world. The unit briefs about the overview of cyber security, how it is different from the information security. The later part of the unit focuses on various types of prevalent cyber threats, cyber crimes, cyber laws and security barriers.
- **Unit-11:** This unit familiarizes the learners about various vulnerable information on the internet such as, malicious software, wireless security challenges, hackers and computer crimes etc. The later part of the unit briefs on the various measures for securing the business or the network transactions along with their various ways of enforcement.
- **Unit-12:** This unit makes the learners aware of the IT Act 2000 along with its various amendments and provisions over time. After studying this unit learners will also be able to understand about the digital signatures, their procedure, working and legal position, cyber crimes, Appellate tribunal, encryption etc.

UNIT 10 CYBER SECURITY

Structure

10.0 OBJECTIVES

After completing this unit, you will be able to:

- differentiate between information security and cyber security;
- understand basic terminologies related to cyber world;
- understand cyber threats and its types; and
- understand cyber crime and law.

10.1 INTRODUCTION

Nowadays usage of smart phone and gadgets is a common thing. It is one of the most noteworthy stuff that is required to be taken under consideration before deeply looking into cyber and its usages. In present scenario cyber

and it's security becoming an essential component of our life because all the data pertains to testimonials, health information, personal information, financial information are stored in the internet and web which in present scenario we call it a cloud. Putting information on virtual platform make all of us familiar all around the world to transform how we connect with others, organize the flow of things, and share information.

It is a place where the data will stay forever but it is not that secured until security is provided to it. In the present scenario Artificial intelligence (AI) has been introduced mutually, AI and the Internet of Things (IoT) will transform both the Internet and the global economy. Within the next five years, we can anticipate AI and Machine learning (ML) to become imbedded in all forms of technology that incorporate data exchange and analysis.

Most of us are always connected to internet each day via smart phones, laptop, home router, smart TV, high end cars, DVR and camera etc., While being connected to internet gives us the prospect to shop online, watch a movie, enjoy music, use maps, search online, pay our bills etc., but with the advent of IoT (Internet of Things) even more gadgets are getting connected like bulbs, thermostat, air conditioners etc. Unfortunately, many of these connected devices will not be designed with security in mind leading to new cyber problems for everyone.

Computer security and cyber security are the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption of the services they make available. Cyber security is becoming an imperative characteristic of life and the reason behind this kind of approach is nothing but the development of technical reliance. Cyber Security is a specialized field in Information Technology (IT) which is regarded as a sub stream in Computer Science.

This unit on Cyber Security provides aims to equip learners with the knowledge and skills required to look after the computer operating systems, networks and data from cyber-attacks. It has a vast usage in E-commerce both as learning as well as its implementation due to the massive financial implications usage with the help of a technology.

10.2 MEANING OF CYBER SECURITY

Cyber threats are a global risk that governments, the private sector, non-governmental organizations – and the global community as a whole – must deal with. Computer security, cyber security or information technology security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field is becoming gradually more noteworthy due to the amplified reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including Smartphone, televisions, and the various devices that constitute the "Internet of things".

Today's world is more about the e-commerce in which precautionary measure need to be taken to safeguard ourselves with a cyber. Keeping in mind cyber security is the way of practicing or rather protecting systems, networks, and programs from digital attacks. These cyber-attacks are frequently aimed at accessing, changing, or destroying susceptible information; extorting money from users; or interrupting normal business processes. Implementing effective cyber-security measures is predominantly challenging nowadays because there are more devices than people, and attackers are becoming more innovative in using state-of-art tools in order to indulge in malpractices and threatening electronically.

10.2.1 Cyber Security Impact On E-Commerce

Cyber security is that part of protection within a business, or organization that is focused on enabling the authorized use of IT systems, at the same time as preventing unauthorized access. The main aim of cyber security is to help make the business more successful. This can involve strategies that enhance confidence with shareholders, customers and stakeholders, through to prevent damage to the business brand, actual losses and business disruptions. Cyber security should be applied to computing devices, such as desktops, servers, laptops, notebooks, smart phones and networks. The field includes all the processes and mechanisms by which digital equipment, information and services are protected from un-intended or unauthorized access, change, or destruction and are of growing importance due to the increasing reliance on computer systems in most societies. Professional cyber security consultants note that it is very rare to find an organization whose data is not compromised in some way. In cyber security circles the acronym C.I.A. sums up the major ways in which data can be at risk.

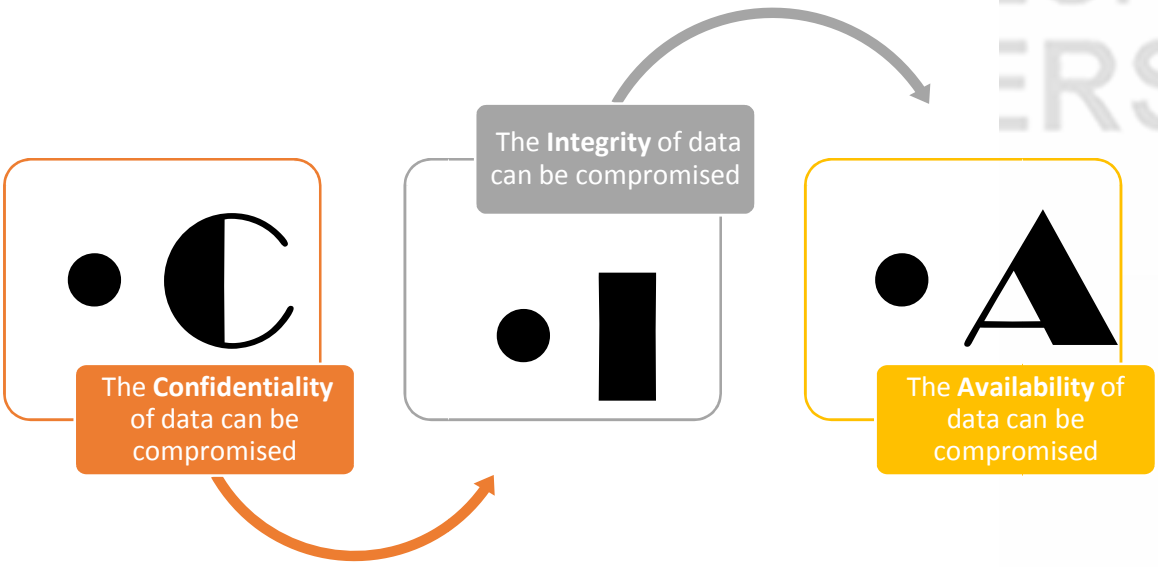


Fig 10.1: C.I.A.

Any three can cause massive fallout to business, particularly those that conduct some of their business online. As cyber security grows in importance in many organizations, professionals that understand how cyber security

objectives interface with broader organizational goals will be increasingly important.

10.2.2 Cyber Security Relevance

Cyber Security is particularly relevant to the following:

- Enabling the safe use of internet connected services, smart devices & communication systems.
- Enabling the safe use of all IT controlled business functions, critical national infrastructures.
- Detection and prevention of unauthorized access.
- Availability of IT systems and Cloud services.
- Secure storage of customers' private and intimate information and data.
- Legal and regulatory compliance.

The content covered in this unit will provide enough detail to understand the role of cyber security and other related security functions within the existing world.

10.3 INFORMATION SECURITY V/S CYBER SECURITY

These two words "Cyber Security" and "Information Security" are generally used as synonyms in security terminology, and create a lot of confusion among security professionals. Some of information security professionals think that cyber security is subset of information security while others think the opposite. So, to clear this confusion, let's start with data security. Data security is all about securing data. Now another question arises here is to the difference between data and information. Not every data can be information. Data can be called as information when it is interpreted in a context and given meaning. For example, "14041989″ is data. And if we know that this is Date of Birth (DOB) of a person, then it is information. So, Information means data which has some meaning, and Information security (also known as InfoSec) is all about protecting the information, which generally focus on the confidentiality, integrity, availability (CIA) of the information. The components of the CIA are:

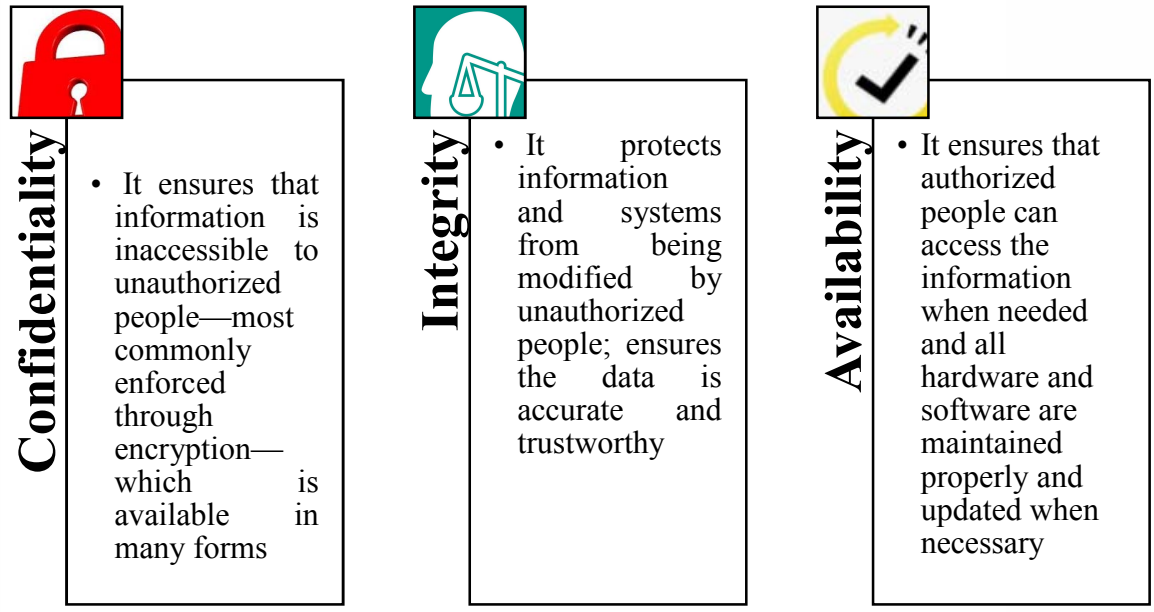


Fig 10.2: Components of the CIA

The CIA combination has become the de facto standard model for keeping the organization secure. The three fundamental principles help build a vigorous set of security controls to preserve and protect your data.

Information security ensures that both physical and digital data is protected from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. Information security differs from cyber security in that InfoSec aims to maintain the security of data in any form. Whereas cyber security protects only digital data i.e., cyber security is about securing things that are vulnerable through ICT. It also considers where data is stored and which technologies are used to secure the data i.e., Cyber security is a subset of information security, and it is the practice of defending your organization's networks, computers and data from unauthorized digital access, attack or damage by implementing various processes, technologies and practices.

One more comparison need attention i.e., Cyber Security and Computer Security, both terms are distant apart. Though both are related and sounds alike, but they are two different terms. Computer security generally includes the security of computer parts like computer hardware and it also deals with the backup of the information stored in the computer, whereas Cyber is a lot more complicated and wider field. It deals with all the threats that can be caused in the Cyber (computer- online and offline) world. Let it be viruses, stealing your personal information, frauds caused by cyber criminals and many more things are taken into consideration. If your business is starting to develop a security program, information security is where you should first begin, as it is the foundation for data security.

10.4 BASICS OF CYBER WORLD

As we know that Cyber security's history began with a research project during the 1970s, on what was then known as the ARPANET (The Advanced Research Projects Agency Network). A researcher named Bob Thomas created a computer program which was able to move ARPANET's network, leaving a small trail wherever it went. The Cyber World, or cyberspace, is more than just the Internet. It refers to an online environment where many participants are involved in social interactions and have the ability to affect and influence each other. People interact in cyberspace through the use of digital media.

10.4.1 Internet and World Wide Web

Now, the next level of understanding for cyber security requires understanding the difference between Internet and WWW (World Wide Web). Most of the people use the words Internet and WWW interchangeably. In fact, they don't see any difference between the two. Only some of the curious folks ask about the difference between Internet and WWW. They wonder if both these things are same. If not, then what are the differences between the two? The quick answer is that technically Internet and WWW are not the same things, and in this section, we will understand the major differences between these two terms.

The Internet: Internet is a massive network of networks. It is essentially an interconnection between millions of smaller computer networks scattered around the globe. These networks are connected with each other by the means of over ground cables, underground cables, satellite links and sub-oceanic cables etc. The word "Internet" actually refers to the entire hardware infrastructure present in the network. Such hardware includes computer systems, routers, cables, bridges, servers, cellular towers, satellites and other pieces. All these pieces of hardware operate under the Internet Protocol (IP). Different computing devices in the Internet are identified by their IP addresses.

World Wide Web (WWW): In the course of life, when people say "Internet", most of the time they actually refer to the World Wide Web or the WWW. The WWW is the collection of all the information that is available in the Internet. So, all the text, images, audio, videos online forms the www. Most of this information is accessed through websites and we identify websites by their domain names. There is huge amount of information available in the WWW. Only a tiny part of this information is searchable through popular search engines like Google. However, most of the information lies in the Deep Web and Dark Web. WWW uses http protocol to access the information from various servers. Information is sent as web pages which are organized in the form of websites. Various web pages are interlinked with each other through hyperlinks. Web pages and other pieces of information in WWW are identified by their address. The following table lists the major differences between the two terms.

Table 10.1 Differences between Internet and WWW

S.No.	INTERNET	WWW
1.	Internet originated sometimes in late 1960s.	English scientist Tim Berners-Lee invented the World Wide Web in 1989
2.	Nature of Internet is hardware.	Nature of WWW is software.
3.	Internet consists of computers, routers, cables, bridges, servers, cellular towers, satellites etc.	WWW consists of information like text, images, audio, video
4.	The first version of the Internet was known as ARPANET	In the beginning WWW was known as NSFNET
5.	Internet works on the basis of Internet Protocol (IP)	WWW works on the basis of Hyper Text Transfer Protocol (HTTP)
6.	Internet is independent of WWW	WWW requires the Internet to exist
7.	Internet is superset of WWW	WWW is a subset of the Internet. Apart from supporting www, the Internet's hardware infrastructure is used for other things as well (e.g., FTP, SMTP)
8.	Computing devices are identified by IP Addresses	Information pieces are identified by Uniform Resource Locator (URL)

10.4.2 Evolution of World Wide Web (WWW)

This World Wide Web is evolved from web 0.0 web 1.0 web 2.0, web 3.0, and now web 4.0, following are the briefs for each generation:

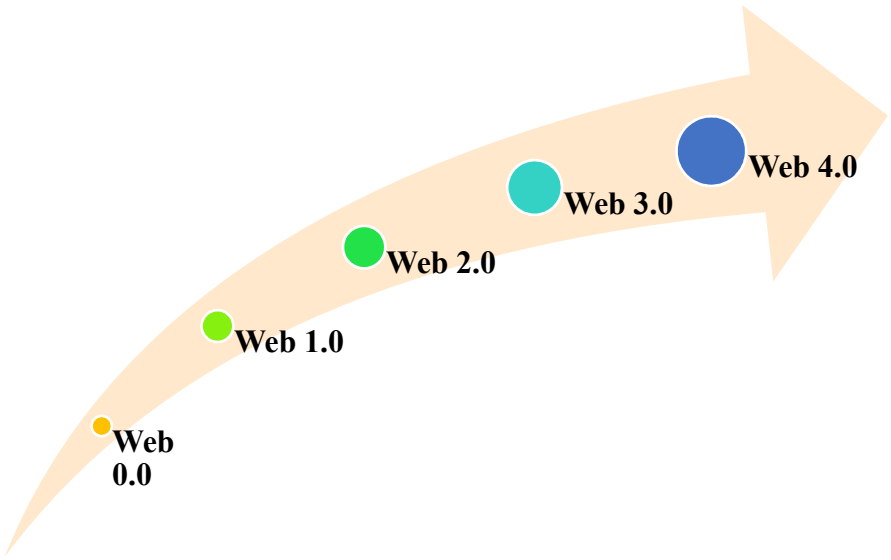


Fig 10.3: Evolution of World Wide Web

1. **Web 0.0 (Developing the internet):** This phase referred to the developmental phase of internet.
2. **Web 1.0 (The shopping carts & static web):** Experts call the Internet before 1999 "Read-Only" web. The average internet user's role was limited to reading the information which was presented to him.

According to Tim Berners-Lee the first implementation of the web, representing the Web 1.0, could be considered as the "read-only web."

3. **Web 2.0 (The writing and participating web):** The lack of active interaction of common users with the web lead to the birth of Web 2.0. This era empowered the common user with a few new concepts like Blogs, Social-Media & Video-Streaming.

4. **Web 3.0 (The semantic executing web):** The Web 3.0 would be a "read-write-execute" web.

5. **Web 4.0 (Mobile Web):** The next step is not really a new version, but is an alternate version of what we already have. We needed to adapt to its mobile surroundings. Web 4.0 connects all devices in the real and virtual world in real-time.

6. **Web 5.0 (Open, Linked and Intelligent Web = Emotional Web):** "The next web". Although Web 5.0 still is in developing mode and the true shape is still forming, first signals are in that Web 5.0 will be about a linked web which communicates with us like we communicate with each other (like a personal assistant). Web 5.0 is called "symbiotic" web. This Web will be very powerful and fully executing. Web 5.0 will be the read-write-execution-concurrency web. Web 5.0 will be about the (emotional) interaction between humans and computers. The interaction will become a daily habit for a lot of people based on neuro technology. For the moment web is "emotionally" neutral, which means web does not perceive the users feel and emotions. This will change with web 5.0 – emotional web. One example of this is www.wefeelfine.org, which maps emotions of people. With headphones on, users will interact with content that interacts with their emotions or changes in facial recognition.

As the bandwidth requirements of WWW are increasing, more and more users are getting connected to the WWW through their smart gadgets and hence the addressing of these gadgets over www is utmost important, the connection less addressing protocol used to track device over WWW is your Internet Protocol (IP)?

IP (short form of Internet Protocol) specifies the technical format of packets and the addressing scheme for computers to communicate over a network. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source. IP by itself can be compared to something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

Upcoming technologies like IoT (Internet of Things), Blockchain, Cloud Computing etc., are result of the continuous increase in the bandwidth requirement of WWW, thus more and more devices are getting connected to the internet/www. Now, to identify these devices uniquely, IP addressing also

requires attention. Thus, to address these increasing number of devices over internet(www) it is required to move from IPV-4 (internet protocol version-4) to IPV-6 (internet protocol version-6), because IPV-6 protocol has capability to address more devices. This IPv6 is the next generation Internet Protocol (IP) standard intended to eventually replace IPv4, the protocol many Internet services still use today. Every computer, mobile phone, and any other device connected to the Internet needs a numerical IP address in order to communicate with other devices. The original IP address scheme, called IPv4, is running out of addresses, because IPv4 uses a 32-bit address scheme allowing for a total of 2^32 addresses (just over 4 billion addresses). Whereas IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons, thus it caters large number of devices and hence quite appropriate for the current technological needs.

10.4.3 Cyberspace

Now because of increasing number of devices over WWW and increasing bandwidth of WWW, more and more users are getting connected to WWW, which increases the possibility of security breach and threats from the cyber world, thus we need cyber security and to understand what is meant by 'cyber security' it is helpful to begin by looking at a definition of cyberspace.

Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our companies, infrastructure and services. Cyberspace can be divided into a multi-layer model comprised of:

1. **Physical foundations:** such as land and submarine cables, and satellites that provide communication pathways, along with routers that direct information to its destination.
2. **Logical building blocks:** including software such as smart phone apps, operating systems, or web browsers, which allow the physical foundations to function and communicate.
3. **Information:** that transits cyberspace, such as social media posts, texts, financial transfers or video downloads. Before and after transit, this information is often stored on (and modified by) computers and mobile devices, or public or private cloud storage services.
4. **People:** It manipulates information, communicate, and design the physical and logical components of cyberspace.

Collectively these tangible and intangible layers comprise cyberspace, which we are increasingly dependent on essential components of daily life. A dependable and stable cyberspace is necessary for the smooth functioning of critical infrastructure, which comprise of software, hardware and networks.

10.4.4 Cyber Security

Cyber security is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide. It can be classified into three categories:

1) **Information Security:** Information security aims to protect the users' private information from unauthorized access and identity theft. It protects the privacy of data and hardware that handle, store and transmit that data. Examples of Information security include User Authentication and Cryptography.

2) **Network Security:** Network security aims to protect the usability, integrity, and safety of a network, associated components, and data shared over the network. When a network is secured, potential threats gets blocked from entering or spreading on that network. Examples of Network Security includes Antivirus and Antispyware programs, Firewall that block unauthorized access to a network and VPNs (Virtual Private Networks) used for secure remote access.

3) **Application Security:** Application security aims to protect software applications from vulnerabilities that occur due to the flaws in application design, development, installation, and upgrade or maintenance phases.

Just to have basic understanding of the cyber world, one should have fundamental acquaintance with the basic terms of cyber space, some of the most important cyber security terminologies that one should know are as follows:

1. **Cloud:** A technology that allows us to access our files and/or services through the internet from anywhere in the world. Technically speaking, it is a collection of computers with large storage capabilities that remotely serve requests.

2. **Software:** A set of programs that tell a computer to perform a task. These instructions are compiled into a package that users can install and use. For example, Microsoft Office is an application software.

3. **Domain:** A group of computers, printers and devices that are interconnected and governed as a whole. For example, your computer is usually part of a domain at your workplace.

4. **Virtual Private Network (VPN):** A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic.

5. **IP Address:** An internet version of a home address for your computer, which is identified when it communicates over a network; For example, connecting to the internet (a network of networks).

6. **Exploit:** A malicious application or script that can be used to take advantage of a computer's vulnerability.

7. **Breach:** The moment a hacker successfully exploits vulnerability in a computer or device, and gains access to its files and network.

8. **Firewall:** A defensive technology designed to keep the bad guys (cyber threats) out. Firewalls can be hardware or software-based.

9. **Malware:** An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include; viruses, trojans, worms and ransomware as covered in a following heads.

    i. **Virus:** A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others. However, in more recent years, viruses like Stuxnet have caused physical damage.

    ii. **Ransom ware:** A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered. For example, WannaCry Ransom ware. For more information on Ransomware, check out our free Ransomware Guide.

    iii. **Trojan horse:** A piece of malware that often allows a hacker to gain remote access to a computer through a "back door".

    iv. **Worm:** A piece of malware that can replicate itself in order to spread the infection to other connected computers.

    v. **Bot/Botnet:** A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A collection of these infected computers is known as a "botnet" and is controlled by the hacker or "bot-herder".

    vi. **DDoS:** An acronym that stands for distributed denial of service – a form of cyber-attack. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).

    vii. **Phishing or Spear Phishing:** A technique used by hackers to obtain sensitive information. For example, using hand-crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

This is just a brief intro of various terms. We will discuss many more concepts in the coming sections of this unit.

10.5 NEED AND CONCEPT BEHIND SECURITY

To help and explain "why security knowledge is so important?" let's first establish the baseline of how daily life operates for most of us. "There aren't many careers left that aren't based on technology, nowadays even teachers in

classrooms are using Smart boards, and many a times someone who comes to your home to do contract work will whip out a smart phone or tablet and add information to an app on the spot, something as small as clicking attachments in emails without knowing if they are safe or there are many more incidences where we need to understand that how such things can affect our security. The mistakes that cause the most damage at companies are security related, of course, security concerns don't stay at work.

We need to understand that "how basic security knowledge can help any career?" Aside from simply not clicking suspicious email attachments, there are things nearly all employees can do to enhance company security and make themselves more valuable workers. Within any role in the organization, learning about security can help an individual understand the risks and make informed decisions for their key stakeholders, here are a few examples:

- In sales, reassure customers of an organization's security posture.
- In corporate communications, you should assess in the context of business reputation and brand trust.
- The legal team should ensure that the right security clauses are built into supplier and customer contracts.
- Regarding HR and/or security, know what's needed for better security awareness and training.
- Product managers should advise on good security features.
- In engineering development, make sure you develop secure code.
- Security professionals should perform reviews and quality assurance tests for functional and security verification.
- Corporate management should ensure that a good security incident response plan is in place to address any vulnerability.

As you can see, it certainly doesn't require being a security professional to contribute to security-related projects and awareness. In fact, the more equipped a workforce is with this knowledge, the less money and time will be lost to security breaches. Based on the analysis of various cyber threats it is found that cyber attackers rely on human error, hackers rely only partly on their security-penetration skills. The other thing they need? People making mistakes. For those who do not work in IT but use computing devices for work, it is necessary to have cyber security training so that they understand how minor mistakes or simple oversights might lead to a disastrous scenario regarding the security or bottom line of their organization. It's a wise step to take on a personal level as well, since even if your mistake was completely unintentional, you won't avoid consequences. No one wants to get fired, especially when you didn't do anything malicious to harm your company, but this is exactly what can happen if you fall victim to an email phishing campaign or other social engineering attack and become the vector by which your company exposes sensitive information. Educate yourself to be suspicious and cautious when it comes to operational security.

10.5.1 Why is Cyber security Important?

In today's attached world, one and all benefits from advanced cyber defense programs. At an individual level, a cyber-security attack can upshot in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Each person relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential for keeping our society functioning. On the other hand educating the public on the significance of cyber security, and build up open source tools which will make the Internet safer for everyone.

Check Your Progress A:

1) What are the various components of the CIA triad?

……

……

……

……

……

2) Why security knowledge is so important?

……

……

……

……

3) What are the various levels of Cyber Space?

……

……

……

……

……

4) Fill in the blanks:

1. ……. is all about securing data.
2. Cloud is a technology that allows us to access our files and/or services through the ……. from anywhere in the world.
3. Exploit A malicious application or script that can be used to take advantage of a computer's ……...
4. Cyberspace is a/an …….. domain made up of digital networks that is used to store, modify and communicate information.
5. Internet is a massive ……. of networks.

10.6 IOT AND CYBER WORLD

Cyber security is becoming an important aspect of life and the reason behind this kind of attitude is nothing but the development of technical dependence. Nowadays having a computer that is full of personal information in every house is a common thing. It is one of the most important things that are required to be taken under consideration that with good kind of threats comes a remedy. The remedy in this case is nothing but the development of the cyber security. It is becoming a necessary component of our life because all the data regarding security information, health information, personal information, financial information are stored in the internet. It is a place where the data will stay forever but it is not that secured until security is provided to it. Most of us are always connected to Internet each day via smart phones, laptop, home router, smart TV, high end cars, DVR and camera etc., while being connected to Internet gives us the opportunity to shop online, watch a movie, enjoy music, use maps, search online, pay our bills etc., but with the advent of IoT (Internet of Things) even more gadgets are getting connected like bulbs, thermostat, air conditioners etc. Unfortunately, many of these connected devices will not be designed with security in mind leading to new cyber problems for everyone. Computer security and cyber security are the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide. Below given are the reasons emphasizing cyber security as more important than ever.

1. **The rising cost of breaches:** The fact is that cyber-attacks can be extremely expensive for businesses to endure. Recent statistics have suggested that the average cost of a data breach at a larger firm is very high. But this actually underestimates the real expense of an attack against a company. It is not just the financial damage suffered by the business or the cost of remediation; a data breach can also inflict untold reputational damage. Suffering a cyber-attack can cause customers to lose trust in business and spend their money elsewhere. Additionally, having a reputation for poor security can also lead to a failure to win new contracts.

2. **Increasingly sophisticated hackers:** Almost every business has a website and externally exposed systems that could provide criminals with entry points into internal networks. Hackers have a lot to gain from successful data breaches, and there are countless examples of well-funded and coordinated cyber-attacks against some of the largest companies in the UK. With highly sophisticated attacks now commonplace, businesses need to assume that they will be breached at some point and implement controls that help them to detect and respond to malicious activity before it causes damage and disruption.

3. **Widely available hacking tools:** While well-funded and highly skilled hackers pose a significant risk to your business, the wide availability of hacking tools and programs on the internet also means there is also a growing threat from less skilled individuals. The commercialization of

cybercrime has made it easy for anyone to obtain the resources they need to launch damaging attacks, such as Ransomware and crypto mining.

4. **A proliferation of IoT devices:** More smart devices than ever are connected to the internet. These are known as the Internet of Things, or IoT, devices and are increasingly common in homes and offices. On the surface, these devices can simplify and speed up tasks, as well as offer greater levels of control and accessibility. Their proliferation, however, presents a problem. If not managed properly, each IoT device that is connected to the internet could provide cybercriminals with a way into a business. IT services giant Cisco estimates there will be 27.1 billion connected devices globally by 2021 so this problem will only worsen with time. With the use of IoT devices potentially introducing a wide range of security weaknesses, it is wise to conduct regular vulnerability assessments to help identify and address risks presented by these assets.

5. **Tighter regulations:** It is not just criminal attacks that mean businesses need to be more invested in cyber security than ever before. The introduction of regulations such as the GDPR (General Data Protection Regulation) means that organizations need to take security more seriously than ever or face heavy fines.

The GDPR has been introduced by the EU to force organizations into to taking better care of the personal data they hold. Among the requirements of the GDPR is the need for organizations to implement appropriate technical and organizational measures to protect personal data, regularly review controls, plus detect, investigate and report breaches.

10.6.1 Cyber Threats

For a cyber-security expert, the Oxford Dictionary definition of cyber threat is a little lacking it's given as the "the possibility of a malicious attempt to damage or disrupt a computer network or system." This definition is incomplete without including the attempt to access files and infiltrate or steal data. In this definition, the threat is defined as a possibility. However, in the cyber security community, the threat is more closely identified with the actor or adversary attempting to gain access to a system. Or a threat might be identified by the damage being done, what is being stolen or the Tactics, Techniques and Procedures (TTP) being used.

To understand just how technology becomes vulnerable to cybercrime or threat, it helps to first understand the nature of threats and how they exploit technological systems. You might first ask why technology is vulnerable at all, and the answer is simple that is trust. From its inception, the protocols that drive internet, by and large, were not designed for a future that involved exploitation, there was little expectation at its birth that we might need to one day mitigate against attacks such as a distributed denial of service (DDoS), or that a webcam you buy off the shelf might need security protocols to prevent it being hacked and used to spy on you. There is much greater awareness today, but even so you can still buy devices that connect to the internet that have poor security measures or no security at all built-in, because up until recently this simply wasn't part of the design scope. In many cases, the idea

that a device might be used for nefarious purposes isn't even considered. And the result is that today cybercrime almost exclusively leverages the lack of security-focused design in everything from your smart phone and web browser through to your credit card and even the electronic systems in your car. The nature of Cyber threats/Cybercrime comes in a variety of forms ranging from denial of service attacks on websites through to theft, blackmail, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransom ware, spyware, social engineering, and even alterations to physical devices (for example, ATM skimmers). It's no surprise then that the sheer scope of possible attacks is vast, a problem compounded by what is known as the attack surface that is the size of the vulnerability presented by hardware and software.

10.6.2 Type of Cyber Threats

In our modern technology-driven age, keeping our personal information private is becoming more difficult. The truth is, highly classified details are becoming more available to public databases, because we are more interconnected than ever. Our data is available for almost anyone to shift through due to this interconnectivity. This creates a negative stigma that the use of technology is dangerous because practically anyone can access one's private information for a price. Technology continues to promise to ease our daily lives; however, there are dangers of using technology. One of the main dangers of using technology is the threat of cybercrimes.

Common internet users may be unaware of cybercrimes, and fall victim of cyber-attacks on a regular basis. Many innocent individuals fall victim to cybercrimes around the world, especially since technology is evolving at a rapid pace. Cybercrimes are any crimes that cause harm to another individual using a computer and a network. Cybercrimes can occur by issues surrounding penetration of privacy and confidentiality. When privacy and confidential information is lost or interrupted by unlawfully individuals, it gives way to high profile crimes such as hacking, cyber terrorism, espionage, financial theft, copyright infringement, spamming, cyber warfare and many more crimes which occur across borders. Cybercrimes can happen to anyone once their information is breach by an unlawful user. Computer security threats are relentlessly inventive. Masters of disguise and manipulation, these threats constantly evolve to find new ways to annoy, steal and harm. We have to equipped with information and resources to safeguard against complex and growing computer security threats and stay safe online. Below mentioned are the few examples of online cyber security threats.

1. **Computer Viruses:** A computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to the computer in the process. It is perhaps the most well-known computer security threat. Carefully evaluating free software downloads from peer-to-peer file sharing sites, and emails from unknown senders are crucial to avoiding viruses. Most web browsers today have security settings which can be ramped up for optimum defense against online threats. But, single

most-effective way offending off viruses is up-to-date antivirus software from a reputable provider.

2. **Spyware Threats:** A **s**erious computer security threat, spyware is any program that monitors your online activities or installs programs without the consent for profit or to capture personal information. While many users won't want to hear it, reading terms and conditions is a good way to build an understanding of how your activity is tracked online. And of course, if a company don't recognize is advertising for a deal that seems too good to be true, be sure that we have an internet security solution in place and click with caution.

3. **Hackers and Predators:** Hackers and predators are programmers who victimize others for their own gain by breaking into computer systems to steal, change, or destroy information as a form of cyber-terrorism. These online predators can compromise credit card information, lock you out of your data, and steal your identity. As we may have guessed, online security tools with identity theft protection are one of the most effective ways to protect yourself from this brand of cybercriminal.

4. **Phishing:** Phishing attacks are some of the most successful methods for cybercriminals looking to pull off a data breach. Masquerading as a trustworthy person or business, phishes attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Antivirus solutions with identity theft protection can be used to recognize phishing threats in fractions of a second.

10.7 CYBER CRIME AND LAW

A commonly accepted definition of cybercrime is a “crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs”. While there are many different definitions of cybercrime, they all have a few key concepts throughout. These key concepts are criminal activity and the use or abuse of computers. With these concepts in mind cybercrime can be easily defined as using a computer to commit a criminal act.

Cybercrimes create an overwhelming task for law enforcement bureaus since they are extremely technological crimes. Law enforcement organizations must have individuals trained in computer disciplines and computer forensics in order to accurately investigate computer crimes or cybercrimes that have been committed. Additionally, many states must modernize and generate legislation, which disallows cybercrimes and outlines suitable penalties for those crimes. Cybercrimes will likely become more frequent with the arrival of advance technologies. It is important that civilians, law officials, and other associates of the justice system are well-informed about cybercrimes in order to diminish the threat that they cause.

Understanding the threat of cybercrimes is a very pertinent issue because technology holds a great impact on our society as a whole. Cybercrime is growing every day because since technological advancing in computers

makes it very easy for anyone to steal without physically harming anyone because of the lack of knowledge to the general public of how cybercrimes are committed and how they can protect themselves against such threats that cybercrimes poses. There are many ways or means where cybercrimes can occur. Here are a few causes and methods of how cybercrimes can be committed on a daily basis.

1. **Hacking:** In other words, can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.

2. **Theft of information contained in electronic form:** This type of method occur when information stored in computer systems are infiltrated and are altered or physically being seized via hard disks; removable storage media or another virtual medium.

3. **Email bombing:** This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.

4. **Data diddling:** It is the changing of data before or during an intrusion into the computer system. This kind of an occurrence involves moving raw data just before a computer can processes it and then altering it back after the processing is completed.

5. **Salami attacks:** This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack. This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace an example is the "Ziegler case "wherein a logic bomb penetrated the bank's system, which deducted only 10 cents from every account and deposited it in one particular account which is known as the "penny shaving".

6. **Denial of Service attack:** It is basically where a computer system becomes unavailable to its authorize end user. This form of attack generally relates to computer networks where the computer of the victim is submerged with more requests than it can handle which in turn causing the pc to crash. E.g., Amazon, Yahoo. Another incident occurs in the past whistle blower site wikileaks.org got a DDoS attack.

7. **Virus / worm attacks:** Viruses are programs that can embed themselves to any file. The program then copies itself and spreads to other computers on a network which they affect anything on them, either by

changing or erasing it. However, worms are not like viruses, they do not need the host to attach themselves to but make useful copies of them and do this constantly till they consume up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers around the world.

8. **Logic bombs:** They are basically a set of instructions where can be secretly be execute into a program where if a particular condition is true can be carried out the end result usually ends with harmful effects. This suggests that these programs are produced to do something only when a specific event (known as a trigger event) occurs. E.g. Chernobyl virus.

9. **Trojan attacks:** The term suggests where a program or programs mask themselves as valuable tools but accomplish damaging tasks to the computer. These programs are unlawful which flaccidly gains control over another's system by assuming the role as an authorised program. The most common form of a Trojan is through e-mail. E.g. lady film director in the U.S.

10. **Internet time thefts:** This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password, an example is Colonel Bajwa's case- in this incident the Internet hours were used up by a unauthorized person.

11. **Web jacking:** This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means. An example of such method was MIT (Ministry of Information Technology) was hacked by the Pakistani hackers whereas another was the 'gold fish' case, site was hacked and the information relating to gold fish was altered and the sum of $ 1 million was demanded.

Cyber terrorism may be defined to be where the deliberate use of disrupting activities, or the risk thereof, via virtual machine, with the purpose to further public, political, spiritual, radical or to threaten any person in continuance of such purposes. Theft crimes include the following:

1. **Credit/Debit Card Fraud:** It is the unlawful use of a credit/debit card to falsely attain money or belongings. Credit/debit card numbers can be stolen from leaky web sites, or can be obtained in an identity theft scheme.

2. **Identity theft:** Identity theft occurs when someone seizes another's individual information without his or her awareness to commit theft or fraudulency. Typically, the victim is led to believe they are revealing sensitive private data to a genuine business, occasionally as a response to an e-mail to modernize billing or membership information etc.

3. **Non-delivery of Goods and Services**: Goods or services that were acquired by individuals online those were never sent.

4. **Phony Escrow Services**: This is where auction participants were persuading by the fraudster where he or she will recommend the use of a third-party escrow service to help the exchange of money and merchandise. The victim is unmindful the impostor has deceived a legitimate escrow service the victim sends payment or products to the phony escrow and obtains nothing in return.

5. **Ponzi/Pyramid method**: This is where investors are lured to capitalize in this falsified arrangement by the promises of irregularly or abnormally high profits but none of the funds are actually made by the so called "investment firm".

Cybercrimes will always be an ongoing challenge despite the advancements being made by numerous countries. Most countries have their own laws to combat cybercrimes, but some doesn't have any new laws but solely relies on standard terrestrial law to prosecute these crimes.

In response to these absolutely complex and newly emerging legal issues relating to cyberspace, cyber law or the law of Internet came into being. The growth of cyberspace has resulted in the development of a new and highly specialized branch of law called cyber laws i.e. laws of the internet and the World Wide Web. Cyber law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of netizens in and concerning Cyberspace comes within the ambit of Cyber law.

Simply we can say that cybercrime is unlawful acts wherein the computer is either a tool or a target or both, Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2008. Cybercrimes are categorized in two ways:

- **The Computer as a Target**:- using a computer to attack other computers. e.g. Hacking, Virus/Worm attacks, DOS attack etc.
- **The Computer as a weapon**:- using a computer to commit real world crimes. e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc.

Cyber Crime is regulated by Cyber Laws or Internet Laws, in India it is addressed by the Information Technology Act, 2008.

Table 10.2: Snapshot of Important Cyber law Provisions in India

OFFENCE	SECTION UNDER IT ACT
Tampering with Computer source documents	Sec.65 (IT Act)
Hacking with Computer systems, Data alteration	Sec.66 (IT Act)
Publishing obscene information	Sec.67 (IT Act)
Un-authorized access to protected system	Sec.70 (IT Act)
Breach of Confidentiality and Privacy	Sec.72 (IT Act)
Publishing false digital signature certificates	Sec.73 (IT Act)
Sending threatening messages by email	Sec 503 (IPC)
Sending defamatory messages by email	Sec 499 (IPC)
Forgery of electronic records	Sec 463 (IPC)
Bogus websites, cyber frauds	Sec 420 (IPC)
Email spoofing	Sec 463 (IPC)
Web-Jacking	Sec 383 (IPC)
E-Mail Abuse	Sec 500 (IPC)
Online sale of Drugs	NDPS Act
Online sale of Arms	Arms Act

Until sufficient legal actions can be put in place where individual countries and global ways of persecution criminals, self-protection remains the first line of defense. The everyday individuals and businesses need to make sure they are educated on what to do in terms of prevent in becoming the next victim of cybercrimes. This basic awareness can help prevent potential cybercrimes against them. The only possible step is to make people aware of their rights and duties and further making more punishable laws which is more stringent to check them.

10.8 SECURITY BARRIERS

While there are hard costs associated with security incidents in terms of lost data or ransom paid, executive leadership also needs to be prepared for other business impacts such as brand erosion, loss of customer goodwill, shareholder disappointment and earnings volatility, all of which can incur costs months and even years after an initial security incident. Everyone knows that they need to secure their networks and systems, but enterprises which are lacking IT resources, dwindling budgets and the sheer volume of risk to manage; handling security nowadays has become a seemingly insurmountable task. Consequently, more and more businesses are looking towards Managed Security Service Providers (MSSP) for help. Here are three common security challenges companies face and how MSSPs can help solve them.

1. **Specialized talent shortage**: There is a shortage of qualified IT security staff, making it difficult for management to attract and recruit qualified personnel. Escalating salary requirements further complicate the situation. Consequently, many companies skip some of the security

management basics simply because they don't have the time or staff required to implement these practices, making them prime hacking targets. An MSSP (Managed Security Service Provider) can operate in a variety of capacities and fill in whatever security gap a company may have. This includes not only devising a security and compliance strategy for networks and devices but taking over daily security management. By partnering with an MSSP, not only do you have access to a dedicated and specialized workforce, but you also benefit from a team of experts that understands the dynamic security landscape and the latest threats. Just as you would depend on a CPA (Certified Public Accountant) to manage your tax filing because of their knowledge of tax law, an MSSP can provide a level of security expertise that is hard to obtain on your own.

2. **Prioritizing risk:** There's no such thing as perfect protection, rather, it's a matter of appropriately managing risk and making a conscious decision about what to do, and perhaps more importantly, what not to do. For example, while you may be dedicated to building a digital fortress with multiple levels of security, the sheer volume and variety of threats make it difficult to assess your current vulnerabilities and to plan an appropriate course of action. An MSSP can identify your security vulnerabilities and compliance requirements and help you implement a plan that's unique to your organization and business situation. From there, you have two options. Your IT team can execute the security plan or you can leverage the MSSP to manage your day-to-day security needs. For example, at Century Link, we help our customers efficiently manage risk by creating a customized security plan, including threat intelligence, detection and response for a myriad of security concerns.

3. **Managing security expenses:** While buyers are spending more than ever on security-related hardware and software, many companies are still exposed and inadequately prepared for a security incident. Simultaneously, buyers are also under pressure from management to reduce spending and provide more predictable operating expenses. But, there is good news. Effective preventive measures aren't necessarily cost prohibitive. An MSSP can help you spend your security dollars smarter by focusing your spending on the priorities that will have the most impact on your security and compliance posture. With a managed security approach, you transfer the cost of ownership, thereby reducing the need for capital investments. You'll gain a predictable OpEx model that is easier to forecast and budget, especially important when IT budgets are expected to remain flat.

Customers who leverage Managed Security Services are able to move from a reactive stance to a proactive security strategy against a rapidly changing threat landscape. Today's reality is that you need to operate with the assumption that your organization will be breached. However, by partnering with an MSSP, you benefit from "strength in numbers" from an intelligence perspective and increase the likelihood you can stay one step ahead of potential hackers. In this modern age, it seems almost impossible to avoid being a victim of cybercrime, with all the advancements in technology which make it easy for someone to perform cybercrimes.

In light of this, there are some ways however to avoid becoming a victim of cybercrime. Most internet browsers email service, and Internet providers provide a spam-blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails, from getting to your inbox. However, every user must ensure to turn them on and do not turn them off whatsoever. Also, users must install and keep up-to-date antivirus programs, firewalls and spyware checkers. Along with keeping them up to date, users must make sure that they run the scans regularly. There are many companies out there that provide free software, but there are other you can purchase, along with that of the many produced by the leading companies' providers; in addition, those companies provide free version of their paid or subscription antivirus software. Encryption of information that you do not want anyone to have unauthorized access to is a good way to avoid some cybercrimes; information such as password and credit card information for example. Encryption software runs your data through encryption algorithms to make it unintelligible to anyone who tries to hack into your computer.

Another good precaution is to be weary of who you divulge your personal information to. Try to avoid unknown websites, in particular those that ask for your name, mailing address, bank account number or social security number. When doing online shopping make sure website is secure, look for URLs that starts with "https" and/or have the Trustee or VeriSign seal.

Fig 10.1: Truste & VeriSign Symbol of Secure website

If you do not see these anywhere on the site, you run the risk of submitting credit card information and other personal information to a site that maybe a fraud. Another way to avoid being a victim of cybercrimes is to avoid being susceptible to common frauds, such as inherences letter, letter asking for your help in placing large sums of money in overseas bank accounts, foreign lotteries, and phony sweepstakes. Those mentioned activities are all methods used by cyber criminals to get your personal information and money. If it sounds too good to be true, it probably is.

Educate children about the proper use of the computer and internet and make sure to monitor their online activities at home and school alike. They should only have access to a computer located in a central area of your home and you should regularly check all browser and email activity. A wise thing is to

use parental control software that limits the type of sites the user can gain access to. In schools, there should be restricted websites and other user restrictions that will help protect the user and entity from cybercrime. Likewise, companies should educate and have written policies governing the workplace pc and its network use to diminish the risk of cybercrime against the company. One definite way to ensure that one don't fall victim of cybercrimes is to disconnect the computer entirely from the internet. If there is no network, then one don't have to worry about any cyber-attacks. However, this option is not the most viable one in our interconnected society. The truth is, it is up to you to take the necessary precautions to avoid potential cybercrimes.

Check Your Progress B:

1) What do you understand by Salami Attacks?

……

……

……

……

2) What are cybercrimes? Explain the various categories of cybercrimes.

……

……

……

……

……

3) Give examples of important cyber law provisions in India.

……

……

……

……

……

4) What is identity theft?

……

……

……

……

10.9 LET US SUM UP

In this modern age, it seems almost impossible to avoid being a victim of cybercrime, with all the advancements in technology which make it easy for

someone to perform cybercrimes. In light of this, there are some ways however to avoid becoming a victim of cybercrime. Most internet browsers email service, and Internet providers provide a spam-blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails, from getting to your inbox. However, every user must ensure to turn them on and do not turn them off whatsoever. Also, users must install and keep up-to-date antivirus programs, firewalls and spyware checkers. Along with keeping them up to date, users must make sure that they run the scans regularly. There are many companies out there that provide free software, but there are other you can purchase, along with that of the many produced by the leading companies' providers; in addition, those companies provide free version of their paid or subscription antivirus software. Encryption of information that you do not want anyone to have unauthorized access to is a good way to avoid some cybercrimes; information such as password and credit card information for example. Encryption software runs the data through encryption algorithms to make it unintelligible to anyone who tries to hack into the computer.

Another good precaution is to be weary of who divulge the personal information to. Try to avoid unknown websites, in particular those that ask for the name, mailing address, bank account number or social security number. When doing online shopping make sure website is secure, look for URLs that starts with "https" and/or have the Trustee or VeriSign seal. If one do not see these anywhere on the site, there run the risk of submitting credit card information and other personal information to a site that maybe a fraud.

Another way to avoid being a victim of cybercrimes is to avoid being susceptible to common frauds, such as inherences letter, letter asking for help in placing large sums of money in overseas bank accounts, foreign lotteries, and phony sweepstakes. Those mentioned activities are all methods used by cyber criminals to get personal information and money. If it sounds too good to be true, it probably is.

Educate children about the proper use of the computer and internet and make sure to monitor their online activities at home and school alike. They should only have access to a computer located in a central area of your home and you should regularly check all browser and email activity. A wise thing to is to use parental control software that limits the type of sites the user can gain access to. In schools, there should be restricted websites and other user restrictions that will help protect the user and entity from cybercrime. Likewise, companies should educate and have written policies governing the workplace pc and its network use to diminish the risk of cybercrime against the company. One definite way to ensure that you don't fall victim of cybercrimes is to disconnect the computer entirely from the internet. If there is no network, then one don't have to worry about any cyber-attacks. However, this option is not the most viable one in our interconnected society. The truth is, it is up to you to take the necessary precautions to avoid potential cybercrimes.

10.10 KEY WORDS

Cyber Laws: Cyber law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of netizens in and concerning Cyberspace comes within the ambit of Cyber law.

Cyber Security: Cyber security is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide**.** The main aim of cyber security is to help make the business more successful.

Cyber Space: Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our companies, infrastructure and services.

Cybercrime: Cybercrimes are the crimes committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. Cybercrimes create an overwhelming task for law enforcement bureaus since they are extremely technological crimes

Hacking: Hacking is the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.

Identity Theft: Identity theft occurs when someone seizes another's individual information without his or her awareness to commit theft or fraudulency. Typically, the victim is led to believe they are revealing sensitive private data to a genuine business, occasionally as a response to an e-mail to modernize billing or membership information etc.

Information Security: Information security also known as InfoSec is all about protecting the information, which generally focuses on the confidentiality, integrity, availability (CIA) of the information. It ensures that both physical and digital data is protected from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.

Logic Bombs: They are basically a set of instructions where can be secretly be execute into a program where if a particular condition is true can be carried out the end result usually ends with harmful effects.

Virus / Worm Attacks: Viruses are programs that can embed themselves to any file. The program then copies itself and spreads to other computers on a network which they affect anything on them, either by changing or erasing it.

Web Jacking: This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on

the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means.

10.11 ANSWERS TO CHECK YOUR PROGRESS

Check Your Progress A:

Q- 4

1) Data security 2) Internet 3) Vulnerability 4) Interactive 5) Network

10.12 TERMINAL QUESTIONS

1) State the differences between Internet and WWW.
2) State the differences between Information Security and Cyber Security.
3) What is Cyber Security? State its importance in the today's digitally connected world.
4) What do you understand by Cyber Threats? Explain its various types.
5) What are the various forms of Cybercrimes?
6) What are the various Security Barriers faced by the companies? How MSSPs can help solve them?
7) What are the various types of Theft Crimes?

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.

UNIT 11 CYBER SECURITY MEASURES

Structure

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.

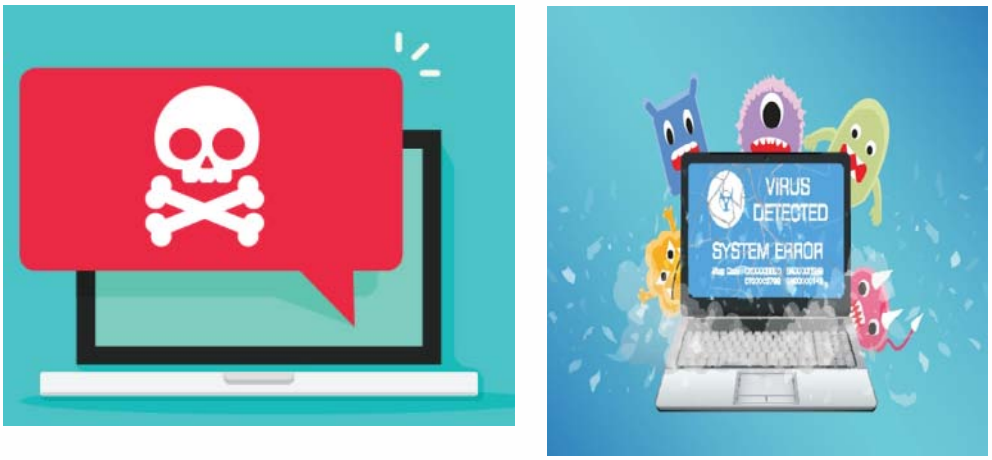


Fig 11.3: Computer Virus

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.

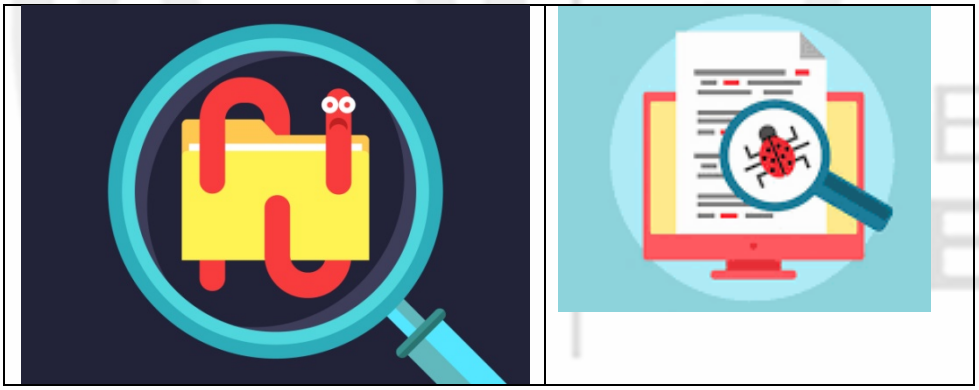


Fig 11.4: Computer Worms

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.

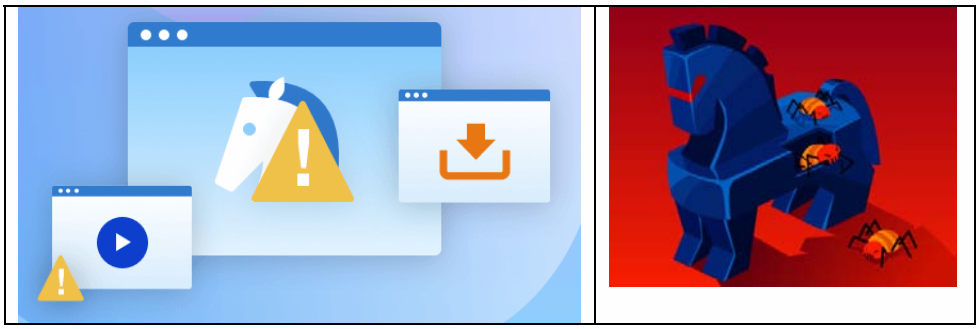


Fig 11.5: Trojan Horse

- **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.

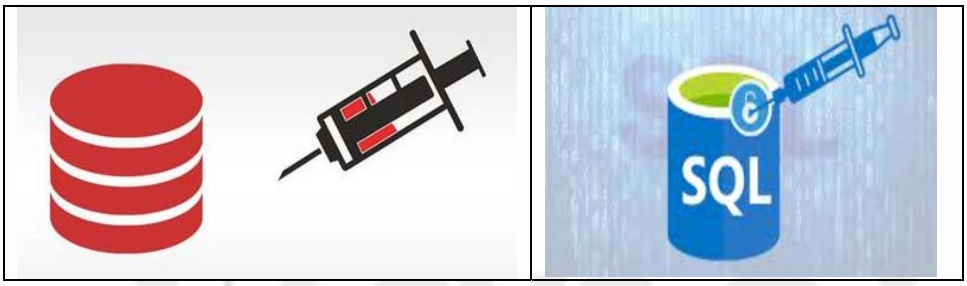


Fig 11.6: SQL Injection

- **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.

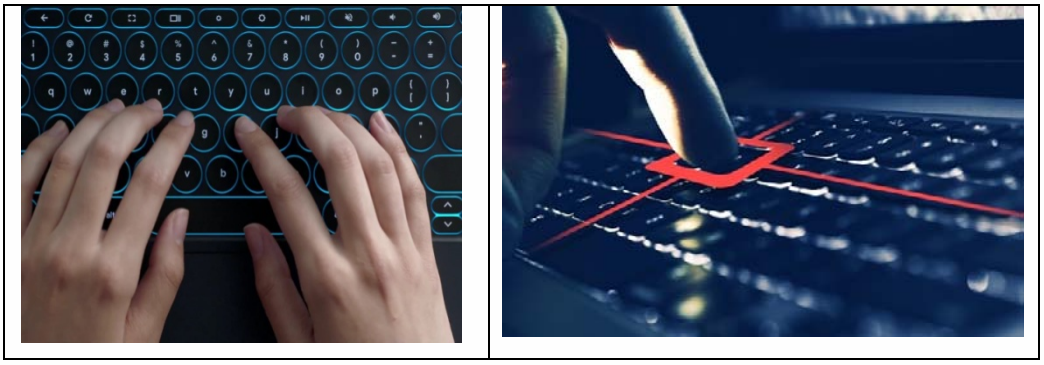


Fig 11.8: Keylogger

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.

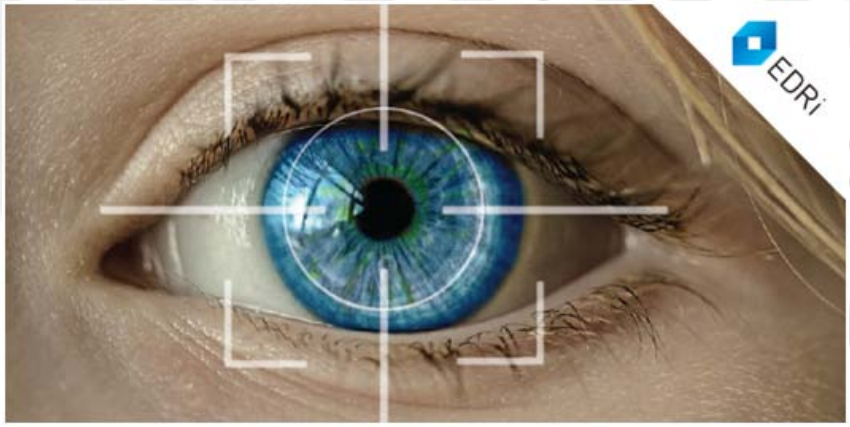
Companies can, wherever necessary, encrypt contact. The password feature found on each Smartphone should be needed for all mobile device users. Some businesses demand that workers only use smartphones from the company. Since BlackBerry devices run on their own safe systems, they are considered safest. 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.

UNIT 12 IT ACT 2000

Structure

12.0 OBJECTIVES

After studying this unit, you should be able to:

- understand the meaning and significance of Information Technology Act;
- explain how IT Amendment Act 2008 came into force;
- describe different provisions of the Act; and
- recognize the meaning of cybercrime and various offences.

12.1 INTRODUCTION

The Information Technology Act was passed as a response to the developments in the IT Sector, to facilitate e-commerce and e-governance, and to control cybercrimes. Internet has become a necessity today and with its increased penetration, clarity was needed in the domain, IT Act was an attempt to provide much needed clarity and direction. This unit discusses various facet of IT Act 2000 and IT Amendment Act 2008.

12.2 DEFINITION

The Information Technology Act, 2000 is the law pertaining to information technology. IT Act, 2000 was the result of passing of the IT the Bill by both the houses of Parliament. The Act is grounded on the United Nations Commission on International Trade Law (UNCITRAL). It deals with E-commerce and cybercrimes. It is, *"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce"*. The Act came into force on 17.10. 2000.

12.3 FORMULATION OF IT ACT 2000

The advent of internet and then the growth in internet-based business transactions necessitated the formulation and implementation of law to regulate the field. The digital technology has transformed our lives, more and more individuals and businesses are adopting it and are conducting several activities with help of it. Before the formulation of IT Act 2000, the overall environment was of apprehension. Individuals and businesses were aware of the advantages this digitalisation brought along, but at the same time they were hesitant to conduct activities, especially monetary transactions owing to the lack of a legal framework which would protect them from some untoward incidents. To match steps with the strides being taken in digital world, the UNCITRAL adopted the Model Law on Electronic commerce in the year 1996. India was also a signatory to this and hence was expected to introduce laws as per the Model Law. Keeping in view, these factors the IT Bill was introduced to facilitate E-commerce as well as E-governance.

The IT Bill was drafted in the year 1998. Then the bill was then put in front of Parliamentary standing committee wherein, certain modifications were suggested. Finally, the IT Ministry suggested some changes and the approved modifications were retained in the bill and the rest were discarded. The bill was approved by the Union cabinet and then both the houses of Parliament. The President of India also provided his assent to the Bill and it became an Act that came into force on 17th October, 2000. The IT Act, 2000 brought in amendments into the Indian Penal Code 1860, the Indian Evidence Act 1872, Bankers Book Evidence Act 1891 and the Reserve Bank of India Act 1934, thereby incorporating the issues related to crimes and evidences based on

electronic mode and to address the need for regulations pertaining to electronic transfer of funds.

12.4 AMENDMENTS IN IT ACT 2000

The Information Technology Act was enacted in the year 2000 to bring in the necessary changes for growth of digitalisation and e-commerce transactions, and ensure safety and security of such transactions, thereby preventing crimes. The act was then amended to account for the developments in the domain, these amendments were passed by both the houses of Parliament in 2008 and received President's assent on 5th February, 2009, thus becoming the Amendment Act. It introduced various positive developments. It was seen as an effort by the Government of India to create a policy that is able to maintain pace with the evolving technology. The Indian Computer Emergency Response Team (CERT-In) is responsible for administration of the Act. The amendment attempted to fill in the gaps left by the earlier Act, and address the security concerns.

The Act was the need of the hour as with increasing digitalisation, the crimes in the digital space or with the help of digital aids also proliferated. Sending/sharing offensive content, phishing, identity theft, frauds, etc. were crimes which had to be brought within the ambit of penal provisions. All these factors led to the amendments in IT Act 2000, thus paving the way for IT Act 2008. The IT Act 2008 revolutionized the cyber law framework of the nation. The Act addressed various issues such as incorporating electronic signature, inclusion of greater number of cyber offences, addressing the concerns pertaining to data protection, privacy, and also dealt with the issues related to use of digital/cyber medium for terrorism.

12.4.1 Amendment Act, 2008 IT Act 2008

The significant contributions of the Amendment Act 2008 are as follows:

- The Act introduced several definitions to bring in more clarity and make it more inclusive:

  i) Electronic signature "means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature"

  ii) Communication Device "means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image."

  iii) Cyber cafe "means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public."

  iv) Cyber Security "means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction."

v) The Act also revised the definition of "Intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes. (Substituted vide ITAA-2008)".

- The Act also brought in changes while addressing the penalties and compensations for damage to computer, computer system, etc. If an individual "destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage; he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."
- Computer Related Offences inserted sections relating to "punishment for sending offensive messages through communication services". It further said, "any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment".

Several other changes were also introduced. These major changes have been discussed in upcoming sections.

Check Your Progress A

1. What was the need for IT Act 2000?

   .....

   .....

   .....

   .....

   .....

2. What prompted the amendments in IT Act, 2000?

   .....

   .....

   .....

   .....

   .....

3. Fill in the blanks:

   i) The IT Act came into force on_____.

   ii) IT Act 2000 was amended in the year _____.

iii) The _____is responsible for administration of the Act.

iv) _____means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image

12.5 DIGITAL SIGNATURE & ENCRYPTION

Under the provisions of IT Act 2000, digital signature may be used by any subscriber for the purpose of authentication of an electronic record. The electronic record is authenticated with the help of "*asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record*. (Section 2(1)(p) of the Information Technology Act, 2000)."

Traditionally, the signature by an individual on any document helps in authentication of the document and provides an assurance to the receiver regarding its trustworthiness. This is possible in case of a paper-based document, but in case of electronic document, just mentioning the name at the end of document or email provides almost no reassurance regarding its authenticity. The IT Act, 2000 recognizes public key cryptography for the safeguarding of electronic documents. The Section 3 of the Act further provides a user the power for authentication of an electronic record by affixing his digital signature. The authentication process will apply "asymmetric crypto system and hash function that envelops and transforms the initial electronic record into another record". The electronic record can be verified by any other person who is in the possession of the public key. Furthermore, every subscriber has a private as well as a public key which are unique to him and which constitutes a functioning key pair. The creation of digital signature requires application of encryption to specific information. The process involves following steps:

- The message that has to be signed using digital signature is outlined, and then processed with the help of an algorithm called hash function. The processed output thus received is called the hash result which is unique to the message.
- This hash result so produced is encrypted using the private key of the sender. This is the Digital Signature.
- The Digital Signature is then attached to the message which is then transmitted over to the receiver through internet.
- Once the message is received at the receiver's end, he uses the public key of the sender to decrypt the message. If the sender's message is successfully decrypted using his public key and the hash result is computed and compared with the output of the digital signature, then the receiver is assured of the authenticity and integrity of the message.

12.6 ATTRIBUTION

The communication taking place through electronic medium does not have any tangible component. Therefore, it becomes difficult to affix responsibilities and define associations. The term attribution means "the action of ascribing a work or remark to a particular author, artist, or person." The IT Act 2000 (Section 11) lays down the guidelines about how an electronic document can be attributed to the individual from whom it originated. It says that the electronic document will be attributed to the originator under following conditions:

- If the originator himself sent the electronic record
- If an individual who was given the authority by the originator to act on his behalf in respect of that particular electronic record has sent it.
- If it was sent by using information system which was programmed by the originator himself or on his behalf to automatically send the electronic record

For example, if an email was sent to B from A, then A will be the originator of the electronic record and B will be the addressee in this case.

12.7 ACKNOWLEDGEMENT AND DISPATCH OF ELECTRONIC RECORDS

Section 12 of the IT Act deals with the manners in which acknowledgement of the receipt of electronic record may be made and Section 13 of the IT Act discusses the time of receipt of an electronic record.

If the originator of the electronic record has not specified any particular mode of acknowledgement to be given by the receiver regarding the receipt of the record, the acknowledgement can be given by "any communication by the addressee, automated or otherwise" or "any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received." For example, if an individual receives a mail for a meeting, the individual can send a mail to the sender saying thank you for the information, or sends an automated response or shows interest by joining the meeting. These activities show acknowledgement from the receiver end.

Also, in cases where the originator of the electronic record has "stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator." But in cases where the originator has not specified that the electronic record will be binding only upon the receipt of acknowledgement and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by

him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent."

The section 13 of the IT Act talks about dispatch of electronic record. It is stated that, the time at which an individual sends the electronic record and it enters a computer outside the ambit of control of the sender, is the time of dispatch. Also, the place of origin of dispatch is the place of business of the sender and the place of receipt is the place of business of the receiver.

12.8 REGULATION OF CERTIFYING AUTHORITIES

The Information Technology Act specifies that the "Controller of Certifying Authorities" may be appointed by Central Government. The controller of certifying authorities has the authority regarding the regulation of certifying authorities. The Government at the Centre may also appoint Deputy Controllers, Assistant Controllers, other officers and employees as they deem fit.

The authority need to assign tasks and functions to the Deputy Controllers and Assistant Controllers lies with the Controller. The Controller's functions include: supervising the activities of the Certifying Authorities, specifying their duties, certifying their keys, laying down standards for them, taking decisions regarding the requirements pertaining to the desired qualification and relevant experience of the Certifying Authorities, etc. The Controller has to certify the public keys of Certifying Authorities and also has to resolve the conflict of interests between them and the subscribers.

The Controller has the authority for the recognition of foreign Certifying Authority as a Certifying Authority with the prior approval of the Central Government, the Controller may also revoke the recognition if he is satisfied "that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition". The Act also provides that any individual can apply for license to the Controller for the purpose of issuing Electronic Signature Certificates in India. The license may be issued if the concerned person satisfies the requirements laid down by the Central Government and is valid only for the period prescribed by the Central Government. For renewing the license, the application has to be accompanied by prescribed fees and the application has to be made forty five days before the date of expiry of the existing license. The application for license may be approved or rejected depending on the merits of the case and the documents accompanying the application. The Controller has the authority to suspend the license, if he is satisfied after an enquiry that false and incorrect statements have been made by the Certifying Authority and the conditions under which the license was issued have not been complied with, but before revocation the Certifying Authority has to be given a reasonable chance of being heard.

The Controller also has the power for the delegation of any of his powers to the Deputy Controller, Assistant Controller or any other officer. The Controller or any other official, who has been authorised by him, has the authority to start the investigation/enquiry regarding any infringement of the IT Act, any other rules or regulations. They will also have access to: "any computer system, any apparatus, data or any other material connected with such system" for the purpose of information retrieval. Also, "the Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 (43 of 1961), and shall exercise such powers, subject to such limitations laid down under that Act."

In case of the Certifying Authorities, they have to make sure that they are following the procedures and protocols as prescribed by the Act and they also have to ensure that their employees also abide by the procedures and protocols. They are expected to adhere to security protocols and use resources which are secure from malicious attacks. They also have to display the license at a conspicuous place within their premises and in case the license is suspended or revoked; they are expected to submit it immediately. It also has to adhere to the disclosure norms so as to maintain sanctity of the process and in case of a situation where in the integrity of their computer systems may be affected; they should notify the concerned stakeholders.

12.9 DIGITAL SIGNATURE CERTIFICATES

The IT Act 2000 talks about digital signature certificates which is a digital key which validates and certifies the identity of the person holding it, and is issued by the certifying agencies. The digital signature certificate verifies the authenticity of the electronic record and ensures that it wasn't altered during the transit. The important characteristics of digital signature certificates are:

- These certificates help in authentication of the message source as the ownership is bound to a specific user.
- They help in providing an assurance that the message was not altered during the transit.
- Non-repudiation is ensured as the sender can not deny sending a message bearing his digital signature.

Any individual can apply for the issue of digital signature certificate by filling up the form and depositing the required amount of fee (not to exceed INR 25,000). The certifying authority may issue the certificate if it finds the application to be in required order. These certificates can only be issued by certifying authority.

12.10 DUTIES OF SUBSCRIBERS

After the issuance of Digital Signature Certificates, the subscribers are expected to perform certain duties as prescribed by the Act. The subscriber

has to take utmost care to hold the control of the private key which corresponds to the public key listed in the Digital Signature Certificate. It is important that he takes all necessary precautions to avoid the leak of the private key, and in case the private key gets compromised he should immediately communicate this to the certifying authority. The subscriber shall be held liable till the time the certifying authority has been informed regarding the breach.

12.11 PENALTIES AND ADJUDICATION

The Information Technology (Amendment) Act, 2008 added several crimes related to cyber space and also introduces penalties for control of such crimes. With increasing penetration of digitalization, the flow of information has been transformed. While there are myriads of advantages of usage of digital media, it is not untouched by increasing crimes. The cyberspace has removed the barriers of geography and has made knowledge/information volatile. To prevent the misuse of information and thus losses accruing out of it, the IT act introduced penalties. The chapter IX of the IT Act discusses Penalties, Compensation and Adjudication.

The penalties for various offences are as follows:

- **Section 43:** "Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)". This section says, if any individual who is not authorised to access/use a computer, computer system or computer network accesses it ,or extract data from it in any form, introduces virus in it or is responsible for some action rusting in virus attack, disrupts it, tampers it, or destroys , deletes or alters any information contained therein will be held responsible for the payment of damages by the way of compensation to the affected person. The compensation should not exceed one crore rupees. This is also applicable in cases wherein he denies the access to authorised person, provides assistance to other for malicious activities, or steals, conceals or destroys the source code of the computer resource with the intention of causing damages.

- **Section 43 A:** "Compensation for failure to protect data (Inserted vide ITAA 2006, Change vide ITAA 2008)".This section deals with cases of negligence, and says "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected."

- **Section 44:** "Penalty for failure to furnish information, return, etc"

  This section discusses penalties resulting from the failure to furnish information, or record, file return, maintain books of account or records. If an individual who is required by the Act to provide information or

return or report to controller or certifying authority, fails to fulfill the requirement, he will be held, "liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure". If he fails to "file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues" and if he is required by the Act to maintain a book of account or maintain certain records, fails to do so, "he shall be liable to a penalty no exceeding ten thousand rupees for every day during which the failure continues."

- **Section 45:** "Residuary Penalty":

  If an individual acts in opposition to any rule and regulation that has been laid down by the IT Act, for which any specific penalty has not been mentioned in the Act, he will be held liable for the payment of compensation of an amount not exceeding 25000 rupees to the individual who gets impacted by the action or a penalty of an amount not exceeding 25000 rupees.

Adjudication

For adjudication pertaining to the matters discussed in the chapter, Central Government has the power to appoint an adjudicating officer. The "Adjudicating Officer should not be below the rank of a director to the GoI or an equivalent officer of a state". An individual should be appointed adjudicating officer only if he has relevant "experience in the field of IT and legal or judicial experience as prescribed by the Central Government". While imposing penalties or awarding compensation, the adjudicating officer shall give reasonable opportunities for representation and should award compensation or penalise only when he is fully satisfied. The adjudicating officer "shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section (2) of section 58." Section 47 of the Act discusses the factors which should be considered by the adjudicating officer while awarding compensation. It says that the officer should be mindful of the gains of unfair advantage which resulted from the default, "the amount of loss caused to the aggrieved party as a result of the default, and the repetitive nature of the default."

Check Your Progress B

1. What are Digital Signature Certificates?

   .....

   .....

   .....

   .....

   .....

   .....

2. What do you mean by Attribution?

.....

.....

.....

.....

.....

3. Fill in the blanks:

i. The IT Act, 2000 recognizes _____cryptography for the safeguarding of electronic documents.
ii. Section ___ of the IT act discusses Penalty and Compensation for damage to computer, computer system, etc.
iii. Section _____ of the IT Act discusses Residuary Penalty.
iv. The subscriber shall be held liable till the time the certifying authority has been informed regarding the breach. **(True/False)**

12.12 PROCEDURE, WORKING & LEGAL POSITION IN DIGITAL SIGNATURE

Digital Signatures have been recognised by Indian legal system under the guidelines issued by IT Act 2000. The Act was an outcome of increased focus on improving the ease of doing business in India and to bring in necessary changes to facilitate the digital transactions. The digital signature ensures that the electronic record is authentic and the content/message has not been tampered with. The IT Act 2000 talks about Digital Signature, while in the ITAA 2008 electronic signature has been mentioned. Digital Signature has been defined as "authentication of electronic record" which happens as per the procedures laid down by the Act. But the IT Act of 2000 included the use of "asymmetric crypto system, public key infrastructure and hash function", thus making it dependent on limited infrastructure only. The introduction of Electronic Signature in IT Act, 2008; brought in technological neutrality and broadened the ambit by covering digital signature as well as other forms such as biometric. Also, it is important to understand that digital (or electronic) signature is not same as scanned copy of signature or a digitized copy, or any other conventional form of signature, it pertains to the authentication of electronic record as per the procedures laid down by Section 3 of the IT Act.

The digital signatures use Public Key Infrastructure and are created and verified with its help. To encrypt and decrypt these signatures, two keys namely are required: public key and private key. The public key is required to encrypt the data which is then decrypted with the help of private key. The public key is shared but the private key used for decrypting is known only to the possessor of the key. The system is based on cryptography.

The signature of an individual is a representation of his identity. It holds a significant legal position and represents the identity as well as intent of the concerned person. The IT Act provided same legal status to digital/electronic signature as the hand-written signature. The concept is based on UNCITRAL Model Law on Electronic Signatures, 2001. These signatures serve the same purpose as traditional signatures. In the digital world wherein, electronic records are being transmitted, the digital signature ensures the authenticity and legitimacy of the electronic record. They are safer than traditional signatures and can not be forged. It is far more convenient to use digital signature.

12.13 APPELLATE TRIBUNAL

The IT Act 2000 provides for the establishment of Cyber Appellate Tribunal. The Act states: "The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal." The central government also has the power to specify the matters and places w.r.t. which the Tribunal may exercise its jurisdiction.

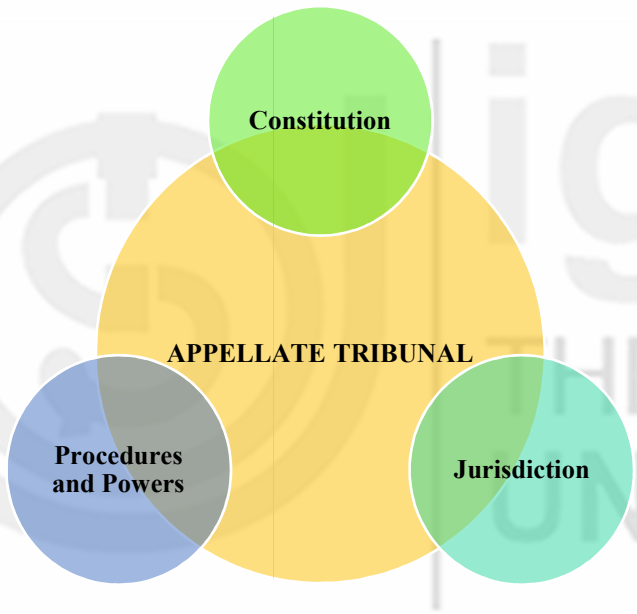


Fig 12.1: Appellate Tribunal

- **Constitution:** The Tribunal shall consist of only one person: The Presiding Officer of the Cyber Appellate Tribunal. The Presiding officer is appointed by the Central Government, and the necessary qualifications for the same are: he will be qualified for the appointment only if he "is, or has been, or is qualified to be, a Judge of a High Court; or is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years." The Presiding officer shall hold the position for 5 years or until he is 65 years of age (Whichever is earlier). The Central Government, in consultation with the Chief Justice of India will be responsible for the selection of chairperson and members of the Tribunal. Also, "The Central Government shall provide the Cyber Appellate Tribunal with such

officers and employees as the Government may think fit" and these people will work under the superintendence of the Presiding Officer.

- **Jurisdiction:** Any individual who is aggrieved pertaining to the orders of a controller or an adjudicating officer may appeal to the Cyber Appellate Tribunal. The appeal has to be filed within 45 days from the date when the order was received by the concerned person. If the aggrieved individual is not satisfied by the decision of Tribunal, he may file an appeal with the High Court.
- **Procedures and Powers:** The Act states that, "The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.". The Tribunal will have same power as civil court (as vested under Code of Civil Procedure, 1908) for the purpose of carrying out its functions in matters such as: summoning and enforcing attendance, requiring the discovery and production of records, receiving evidence, reviewing decisions, etc. The proceedings before the tribunal will be deemed "to be a judicial proceeding within the meaning of sections 193 arid 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973."

12.14 OFFENCES AND CYBER-CRIMES

The advent of internet has transformed our lives. People in every sphere of life are using computers and internet to create, transmit and store information. The information is volatile in nature and is often misused by miscreants, thereby causing harm to others. With increasing penetration of internet and adoption of digital tools and techniques, global connectivity has reached new heights, but at the same time has become even more vulnerable resulting in increased numbers of crimes. To control such malicious activities and deter the miscreants the IT Act was introduced with provisions for addressing these issues. Chapter XI of the IT Act discusses criminal offences which are punishable by fine or imprisonment or both.

Cybercrimes is an umbrella term which includes the criminal activities involving computer/internet/cyberspace. It is basically criminal exploitation of computer and/or internet. These crimes are of sophisticated nature and in these crimes the computer is usually the tool or target or both. It includes:

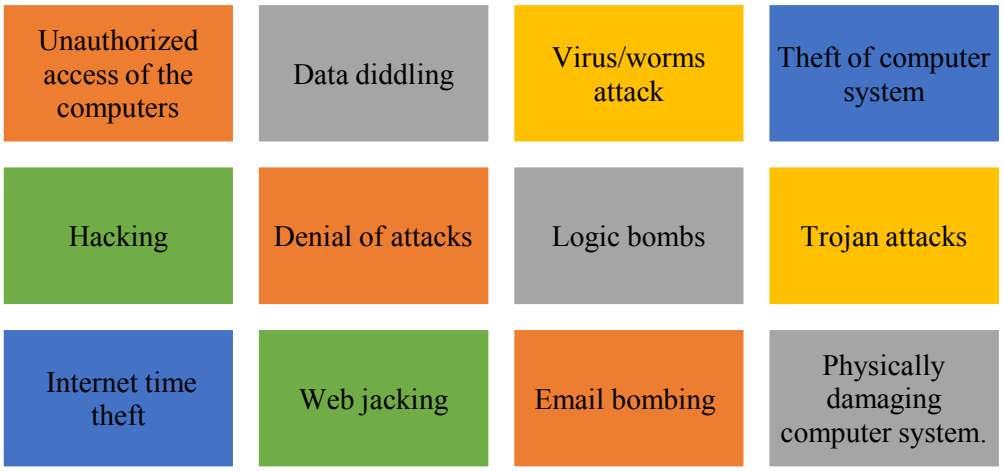


Fig 12.2 : Cyber Crimes

The Indian law does not provide any specific definition of cybercrime, but the term cyber security has been defined, it "means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction." Even though cyber-crime has not been defined in the IT Act but offences and crimes relating to computers and cyberspace have been dealt in detail in the IT Act. Following offences have been included in IT Act:

Table 12.1: Offences and their punishments

Section	Offence	Punishment
Section 65	Tampering with computer source documents	Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
Section 66	Computer related offences	Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
Section 66 B	Punishment for dishonestly receiving stolen computer resource or communication device	imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
Section 66 C	Punishment for identity theft	Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
Section 66 D	Punishment for cheating by personation by using computer resource	Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66 E	Punishment for violation of privacy	Imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
Section 66 F	Punishment for cyber terrorism	Imprisonment which may extend to imprisonment for life
Section 67	Punishment for publishing or transmitting obscene material in electronic form	Imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
Section 67 A	Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form	Imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
Section 67 B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	Punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
Section 67 C	Preservation and retention of information by intermediaries	Punished with an imprisonment for a term which may extend to three years and also be liable to fine.
Section 68	Power of Controller to give directions	Imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.
Section 69	Power to issue directions for interception or monitoring or decryption of any information through any computer resource	Imprisonment for a term which may extend to seven years and shall also be liable to fine.

Section 69 A	Power to issue directions for blocking for public access of any information through any computer resource	Imprisonment for a term which may extend to seven years and also be liable to fine.
Section 69 B	Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment for a term which any extend to three years and shall also be liable to fine.
Section 70	Protected system: Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
Section 70 B	Indian Computer Emergency Response Team to serve as national agency for incident response	Imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.
Section 71	Penalty for misrepresentation	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Section 72	Penalty for Breach ofconfidentiality and privacy	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Section 72 A	Punishment for disclosure of information in breach of lawful contract	Imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.
Section 73	Penalty for publishing[electronic signature] Certificate false in certain particulars	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Section 74	Publication for fraudulent purpose	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

The Act will also apply to contraventions conducted outside India if it involves computer, computer system or computer network based out of India.

12.15 E-SIGNATURE AND DIGITAL SIGNATURE

The IT Act of India discusses two types of signatures:

- Electronic Signature, and
- Digital Signature.

Important points for comparison have been summarised below:

- Section 2(1) (ta) of the IT Act 2008 defines Electronic Signature as: "electronic signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature". The section 2(1) (p) of the IT Act 2000 talks about Digital Signatures and defines it as "digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3" of the Information Technology Act.
- Electronic Signatures are technologically neutral and the act does not specify any particular technology for the purpose of creation of electronic signature while digital signature follows specific technology-based approach. For example, usage of hash functions, use of public key cryptography system, etc.
- Electronic Signature can be biometric, name typed at the end of a mail, digitalized version of conventional signature. Digital signature uses two-way protection system with encryption and decryption.
- Digital Signatures are more authentic than electronic signatures.
- Electronic signatures are used for the purpose of verification of document while Digital Signatures are used for securing the document.
- Digital Signatures have limited validity of maximum three years, while electronic signatures have no such limits on validity.

12.16 ENCRYPTION

A Digital Signature is used for the authentication of an electronic record. These signatures are created and verified with the help of cryptography. The authentication process involves two other processes: Encryption and Decryption.

Encryption involves transformation of simple messages into cipher text while the process of decryption reverses the coded texts into the actual simple message.

Encryption-Decryption has two forms:

- Symmetric Encryption: It is the most basic kind of encryption involving only one secret key for the purpose of encryption and decryption of information. The key is known to both: the sender as well as the receiver of the message.
- Asymmetric Encryption: There are two keys involved in this case for encrypting/decrypting messages: public key and private key or secret key. Section 2(1)(f) of the Information Technology Act 2000 talks about this kind of encryption. The encryption is done using the public key which is known to many but decryption can only be done by the individual who has the private key known to the receiver only. It helps in protecting the digital signature from forgery. Asymmetric encryption is a relatively modern method.

Check Your Progress C

1. What are the different kinds of encryption?

   ……
   ……
   ……
   ……
   ……
   ……

2. Explain the constitution and jurisdiction of Cyber Appellate Tribunal.

   ……
   ……
   ……
   ……
   ……
   ……

3. Fill in the blanks:

   i) Digital Signatures have been recognised by Indian legal system under the guidelines issued by _____.

   ii) _____is the most basic kind of encryption involving only one secret key for the purpose of encryption and decryption of information.

   iii) There are two keys involved in the case of _____for encrypting/decrypting messages: public key and private key or secret key

   iv) The Tribunal shall consist of only one person: The _____of the Cyber Appellate Tribunal.

12.17 LET US SUM UP

The Information Technology Act, 2000 is the law pertaining to information technology. IT Act, 2000 was the result of passing of the IT the Bill by both the houses of Parliament. The Act is grounded on the United Nations Commission on International Trade Law (UNCITRAL). It deals with E-commerce and cybercrimes.

Under the provisions of IT Act 2000, digital signature may be used by any subscriber for the purpose of authentication of an electronic record. The electronic record is authenticated with the help of "*asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record*. (Section 2(1)(p) of the Information Technology Act, 2000)."

The communication taking place through electronic medium do not have any tangible component. Therefore, it becomes difficult to affix responsibilities and define associations. The term attribution means "the action of ascribing a work or remark to a particular author, artist, or person." The IT Act 2000 (Section 11) lays down the guidelines about how an electronic document can be attributed to the individual from whom it originated.

If the originator of the electronic record has not specified any particular mode of acknowledgement to be given by the receiver regarding the receipt of the record, the acknowledgement can be given by : " any communication by the addressee, automated or otherwise" or "any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received." For example, if an individual receives a mail for a meeting, the individual can send a mail to the sender saying thank you for the information, or sends an automated response or shows interest by joining the meeting. These activities show acknowledgement from the receiver end.

The IT Act 2000 talks about digital signature certificates which is a digital key which validates and certifies the identity of the person holding it, and is issued by the certifying agencies. The digital signature certificate verifies the authenticity of the electronic record and ensures that it wasn't altered during the transit.

12.18 KEY WORDS

Attribution: The action of ascribing a work or remark to a particular author, artist, or person.

Digital Signatures: Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Digital Signature Certificate: The digital signature certificate verifies the authenticity of the electronic record and ensures that it wasn't altered during the transit.

Electronic Signature: Authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.

Encryption: Encryption involves transformation of simple messages into cipher text while the process of decryption reverses the coded texts into the actual simple message.

IT Act: An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce.

12.19 ANSWER TO CHECK YOUR PROGRESS

A) i. 17.10. 2000 ii. 2008 iii. Indian Computer Emergency Response Team (CERT-In) iv. Communication Device

B) i. Public key ii. 43 iii. 45 iv. True

C) i. IT Act 2000 ii. Symmetric Encryption iii. Asymmetric Encryption iv. Presiding Officer

12.20 TERMINAL QUESTIONS

1. Write brief notes on following:
   i) Certifying Authority
   ii) Duties of Subscribers
   iii) Appellate Tribunal
   iv) Encryption
2. Differentiate between the following:
   i) Digital Signature and Electronic Signature
   ii) IT Act 2000 and IT (Amendment) Act 2008
3. Explain the process of encryption in Digital Signatures.
4. Explain the process pertaining to Acknowledgement and dispatch of electronic records.
5. What are cyber-crimes?

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.