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.

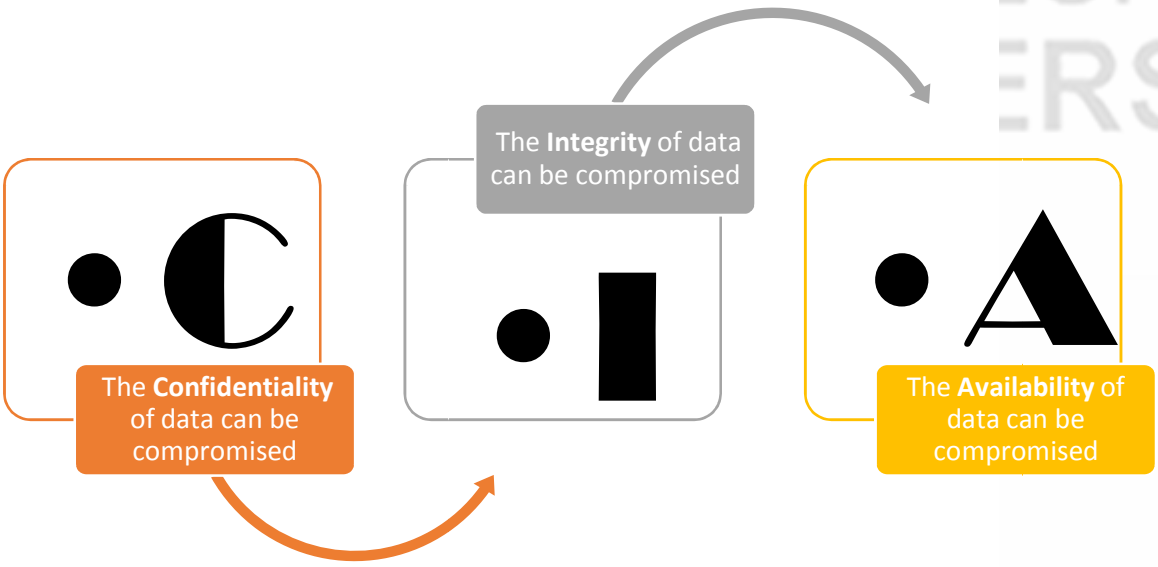

Fig 10.1: C.I.A.

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:

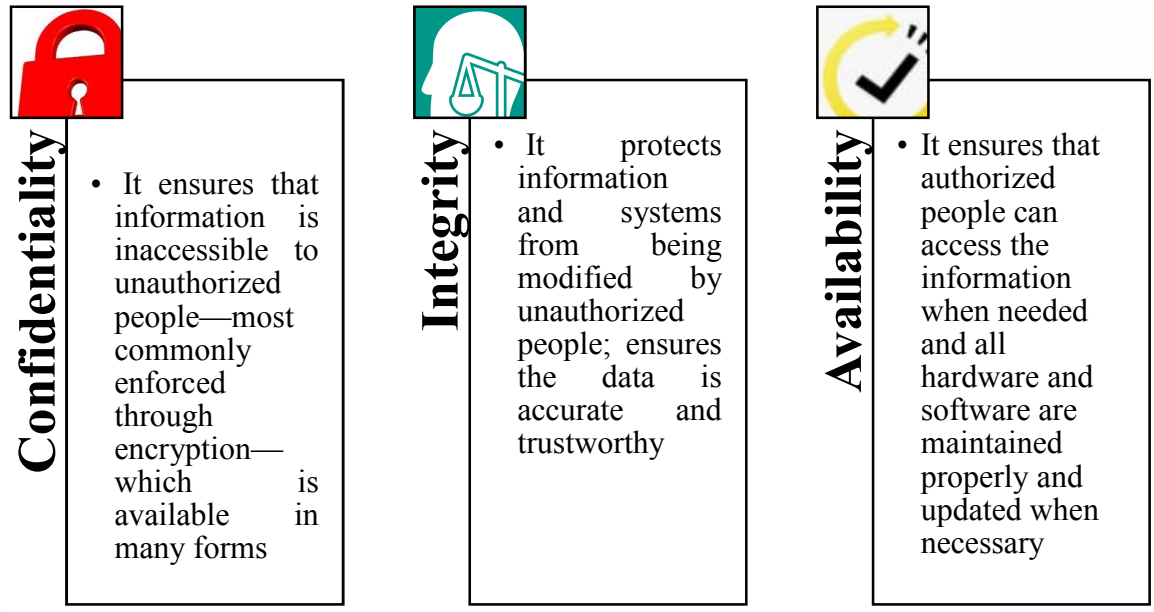

Fig 10.2: Components of the CIA

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:

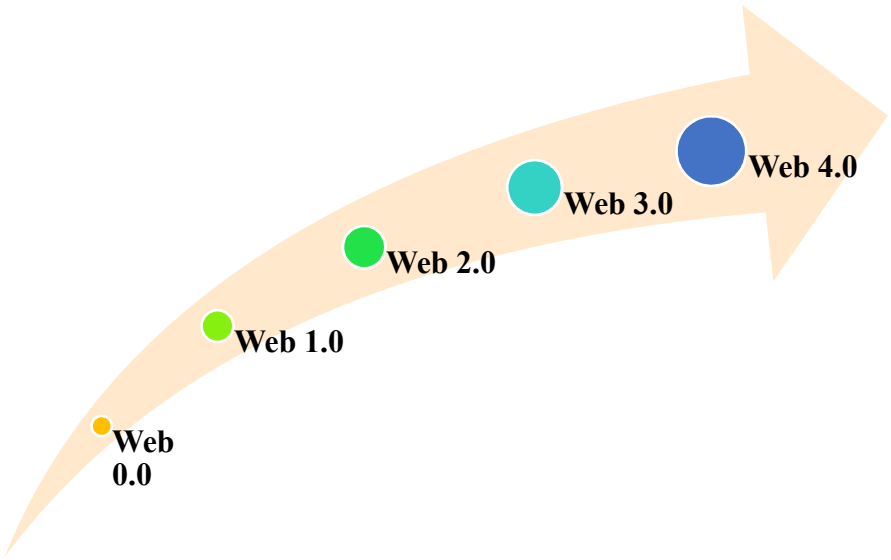

Fig 10.3: Evolution of World Wide Web

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.