UNIT 5 THE CONCEPT OF SECURITY IN CYBERSPACE

Structure

5.1 Introduction
5.2 Objectives
5.3 Cyberspace – Why is it not Secure?
5.4 Why Should We Secure Cyberspace?
5.5 Security Challenges in Cyberspace
  5.5.1 Hacking
  5.5.2 Child Pornography
  5.5.3 Cyber Stalking
  5.5.4 Denial of Service
  5.5.5 Dissemination of Malicious Software (Malware)
  5.5.6 Phishing
  5.5.7 Information Warfare
  5.5.8 Data related
  5.5.9 Network Related
5.6 The Concept of Cyber Security
  5.6.1 Technology’s Answers to Cyber Security
  5.6.2 Cyber Security and Law
5.7 Computer Related or Computer Facilitated Crime
5.8 Application of Basic Criminal law Concepts
5.9 Summary
5.10 Terminal Questions
5.11 Answers and Hints
5.12 References and Suggested Readings

5.1 INTRODUCTION

It will be interesting for us to understand the meaning of ‘cyberspace’ before addressing issues concerning its security.

The word ‘cyberspace’ was coined by William Gibson, a Canadian science fiction writer, in 1982 in his novelette ‘Burning Chrome’ in Omni magazine, and was subsequently popularised in his novel Neuromancer.

Cyberspace should not be confused with ‘internet’. While the internet is the interconnection between millions of computers located around the world, each of them independently managed by persons who have chosen to adhere to common communications protocols, particularly a fundamental protocol suite known as Transmission Control Protocol or Internet Protocol (TCP/IP), which makes it practical for computers to share data even if they are far apart and have no direct line of
Data Security

communication, the term ‘cyberspace’ is often used simply to refer to objects and identities that exist largely within the computing network itself, so that a web site, for example, might be metaphorically said to ‘exist in cyberspace’. According to this interpretation, events taking place on the internet are not therefore happening in the countries where the participants or the servers are physically located, but ‘in cyberspace’.

When we sit in front of a computer and switch it on, something like magic happens before us; if we are correctly connected we can bring up an environment of hypertext with a click of the mouse. It feels like that behind the screen, there is a potentially very huge reservoir of information that is always in the making. Such a reservoir is somewhere, out there. We are certainly aware that people who generate information, and place wherein information resides, are not behind the screen or in the hard drive, but we nevertheless take the computer as a gateway to another place where other people have done similar things. Conceptually, we tend to envision a nonphysical ‘space’ existing between here and there, and believe that we can access that ‘space’ by utilizing computer-based technologies. We send messages to others by e-mail, or talk to others in a chat room. We play an online interactive game as if our opponent (in the game) is right before us, though invisible. By participating in an on-line teleconference, we experience the presence of other conference participants. But where are we? Where are the others with whom we communicate? We seem to communicate in a medium that is not defined, there is a sense of spatiality. Usually, we call this medium ‘cyberspace’, the ‘space’ that seems to open up or shut down as the computer screen is activated or deactivated.

5.2 OBJECTIVES

After studying this unit, you should be able to:
- know the meaning of ‘cyberspace’;
- know the reasons for security concerns in cyberspace;
- explain the need to secure cyberspace;
- describe the specific security challenges to cyberspace;
- explain the concept of Cyber Security; and
- know the distinction between computer related and computer facilitated crime.

5.3 CYBERSPACE – WHY IS IT NOT SECURE?

The TCP/IP protocol suite makes the internet possible. Its most important feature is that it defines a packet-switching network, a method by which data can be broken up into standardised packets that are then routed to their destinations via an indeterminate number of intermediaries. Under TCP/IP, as each intermediary receives a packet intended for a party further away, the packet is forwarded along whatever route is most convenient at the nanosecond the data arrives. So in simple terms, if you desire to deliver a package to a friend, instead of sending it as one whole piece, you send parts of the package through many people who are heading in the direction of the recipient. If one such person carrying part of the package meets another person who is heading to meet the recipient, then this person hands over his parts to the other person, eventually the parts finally reach the recipient. In this model you can see some level of confusion. The package goes all over space before it reaches its final destination; it also exchanges or moves hands.
Another reason for insecurity associated with cyberspace is its end-to-end design. The network is designed in a manner that any form of intelligence, including security interfaces are placed only at the ‘ends’. You may call these interfaces, fire walls, filters, spam killer, diluter, etc. With end-to-end design, the network has minimal control or intelligence to intercept the manner of its usage. Computers within the network are only required to provide the most basic level of service — data transport via the TCP/IP protocols. The network itself is kept simple, incapable of discrimination. Without intelligence imbedded in the network all packets that conform to the protocol are transmitted, regardless of content, regardless of intent, and without any knowledge (or care) of what types of applications or people are utilizing the packets on the ends of the network.

Further, the Internet is not controlled by a single company or agency. The only organization that exerts some level of monitoring of the internet is an international, un-incorporated organization called the Internet Engineering Task Force. A primary activity of the IETF is internet standard-setting. The Internet Standards Process (ISP) is concerned with all protocols, procedures, and conventions that are used in or by the Internet, including the TCP/IP protocol suite.

The technology – packet – switching protocols, the end to end network design and the impossibility of centralized control make computer networks or cyberspace an anarchic ethos. The endeavour is to bring sublimity to the confusion and then, over a period of time, instill control that will assume some checks and provide security to the “network”.

Please answer the following Self Assessment Question.

<table>
<thead>
<tr>
<th>Self Assessment Question 1</th>
<th>Spend 4 Min.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the three main reasons for contributing lack of security to cyberspace?</td>
<td></td>
</tr>
</tbody>
</table>
Data Security

‘cyberspace’ to contribute to economic growth, human development and democratisation, it must be trustworthy and secure. Lack of trust and security jeopardises development goals that could be supported by a trusted cyberspace.

Securing cyberspace is by no means an easy task. Its universal spread, across all nations without the barriers of sovereign controls makes the challenge of monitoring cyberspace even more difficult. It will be impossible to secure cyberspace through law without the application of technology and participation of every individual who accesses cyberspace. The United States Government while implementing its National Strategy to Secure Cyber observes that cyberspace by its very nature is chaotic and beyond the reach of any organized or central control.

Please answer the following Self Assessment Question.

Self Assessment Question 2

What are the specific losses that businesses face on account of an unsecure cyberspace?

............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................
............................................................................................................................

5.5 SECURITY CHALLENGES IN CYBERSPACE

As discussed earlier, cyberspace faces constant threat of creative misuse. How does one ensure to minimize this threat? The best way to begin is by being aware of the kind of cyber threats and then to use this awareness to find means of controlling the violation. This process as you will see, that is, identifying the threat and then adequately protecting against them, is an ongoing process of legislation, technological innovation and co-operation amongst users, on a micro level amongst users and amongst nations at the macro user level. Cyber crimes consist of specific crimes dealing with computers and networks, such as hacking, phishing and the facilitation of traditional crime through the use of computers (child poronography, hate crimes, telemarketing/internet fraud). In addition to cyber crime there is also computer supported crime which covers the use of computers by criminals for communication and data storage. A brief introduction to some common cyber related violations, or cyber crimes as they are more commonly referred to are discussed below:

5.5.1 Hacking

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from Indian legal perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. Some hackers hack for personal monetary gains, such as for stealing credit card information or
transferring money from various bank accounts to their own followed by withdrawal of money. They also indulge in extortion based on information received while hacking a particular network of computer system.

5.5.2 Child Pornography

The Internet is extensively used for sexual abuse of children. As more homes have access to internet, more children are accessing it and this enhances their vulnerability of falling victims to the aggression of paedophiles.

Easy access to pornographic contents readily and freely over the internet lowers the inhibitions of children. Paedophiles lure the children by distributing pornographic material and then pursue them for sexual exploitation. Sometimes paedophiles contact children in chat rooms posing as teenagers or a children of similar age, they win the confidence of these children, then induce them into sexually provocative discussions. Then begins the actual exploitation of children.

5.5.3 Cyber Stalking

There is no universally accepted definition of cyberstalking, the term is used to refer to the use of the internet, e-mail, or other electronic communications devices to stalk another person. Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person’s home or place of business, making harassing phone calls, leaving written messages or objects, or vandalising a person’s property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim’s immediate family; and still others require only that the alleged stalker’s course of conduct constitute an implied threat.

Cyber stalking can be defined as the repeated acts of harassment or threatening behaviour of the cyber criminal towards the victim by using internet services. The *modus operandi* of most stalkers is as follows:

a. Collect personal information about the victim. If the stalker is a stranger to victim, he collects the information from internet resources such as various profiles the victim may have filled in while opening a chat or e-mail account or while signing an account with some website.

b. The stalker may post information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone to obtain sexual services.

c. Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which the victim starts receiving indecent soliciting e-mails.

d. Some stalkers send repeated e-mails asking for various kinds of favours or threaten the victim.

5.5.4 Denial of Service

This is a technology driven cyber intrusion, where by the influencer floods the bandwidth or blocks the user’s mails with *spam* mails depriving the user, access to the Internet and the services provided therefrom. A DoS Attack (as it is commonly known) can be perpetrated in a number of ways. There are three basic types of attack:
Data Security

a. consumption of computational resources, such as bandwidth, disk space, or central processing unit (CPU) time;

b. disruption of configuration information, such as routing information; and
c. disruption of physical network components.

5.5.5 Dissemination of Malicious Software (Malware)

Malware is defined as a software designed to perform an unwanted illegal act via the computer network. It is also loosely defined as software with malicious intent. Malware can be classified based on how they get executed, how they spread, and/or what they do. Some of them are discussed below.

a) **Virus**

The term “computer virus” was first termed by Fred Cohen in 1983 in his Ph.D thesis. A virus is a program that can infect other programs by modifying them to include a possible evolved copy of itself. A virus can spread throughout a computer or network using the authorization of every user using it to infect their program. Every program so infected may also act as a virus and thus the infection grows. Viruses normally affect program files, but in some cases they also affect data files disrupting the use of data and destroying them completely.

b) **Worms**

Worms are also disseminated through computer networks, unlike viruses, computer worms are malicious programs that copy themselves from system to system, rather than infiltrating legitimate files. For example, a mass mailing e-mail worm is a worm that sends copies of itself via e-mail. A network worm, on the other hand makes copies of itself throughout a network, thus disrupting an entire network.

c) **Trojans**

Trojan is another form of Malware, trojans do things other than what is expected by the user. Trojan or trojan horse is a program that generally impairs the security of a system. The program is usually disguised as something else (a benign program) or is masqueraded as a legitimate file that the user would expect to see, or want to load, on the system. The payload of a Trojan is usually delivered as soon as it is opened and usually with devastating results. Trojans are used to create back-doors (a program that allows outside access into a secure network) on computers belonging to a secure network so that a hacker can have access to the secure network. Also, most often trojans are associated with remote access programs that perform illicit operations such as password stealing or which allow compromised machines to be used for targeted denial of service.

d) **Hoax**

Hoax is an e-mail that warns the user of a certain system that is harming the computer. The message thereafter instructs the user to run a procedure (most often in the form of a download) to correct the harming system. When this program is run, it invades the system and deletes an important file.

e) **Spyware**

Spyware invades a computer and, as its name implies, monitors a user’s activities without consent. Spywares are usually forwarded through unsuspecting e-mails with bonafide e-mail i.d.s. Spyware continues to infect millions of computers globally.
5.5.6  Phishing

Phishers lure users to a phony web site, usually by sending them an authentic appearing e-mail. Once at the fake site, users are tricked into divulging a variety of private information, such as passwords and account numbers.

5.5.7  Information Warfare

Information warfare is a kind of warfare where information and attacks on information and its system are used as a tool of warfare. Information warfare may include giving the enemy propaganda to convince them to give up, and denying them information that might lead to their resistance. Information warfare may also include feeding propaganda or even disinformation to one’s own population, either to build support for the war effort or to counter enemy propaganda.

Information warfare may also mean a strategy for undermining an enemy’s data and information systems, while defending and leveraging one’s own information edge. This type of war has no front line; potential battlefields are anywhere networked systems can be accessed—oil and gas pipelines, electric power grids, telephone switching networks, etc.

Information warfare can take countless forms: trains and planes can be misrouted and caused to collide, stock exchanges can be sabotaged by electronic “sniffers” which disrupt international fund-transfer networks, and the signals of television and radio stations can be jammed and taken over and used for a misinformation campaign.

During the Gulf War, Dutch crackers stole information about U.S. troop movements from U.S. Defence Department computers and tried to sell it to the Iraqis, who thought it was a hoax and turned it down. In January 1999, U.S. Air Intelligence computers were hit by a coordinated attack, part of which appeared to come from Russian cracking.

5.5.8  Data Related

Data interception - Hijacking e-mails, interference of an intermediary in the network, may be a prelude to another type of computer crime, typically data modification.

Data modification - Usually done in conjunction with data interception, valid data intended for a recipient is hijacked or intercepted and then is replaced with an erroneous one. This could also apply to illegal tapping into database and altering its contents. Basically, any form of alteration without appropriate authorization falls under this category.

Data theft - Outright stealing of most commonly classified or proprietary information without authorization. This could be the result of data interception. It might also be the unlawful use or possession of copyrighted works such as songs, pictures, movies or other works of art.

5.5.9  Network Related

Network interference - Any activity that causes the operation of a computer network to be temporarily disrupted. Interference implies something momentarily such as Denial of Service Attacks that causes delays in data transmission by using up all available bandwidth. Distributed denial of service, ping of death and smurf attacks also fall under this category.
Data Security

Network sabotage - causing permanent damage to a computer network such as deleting files or records from storage.

Please answer the following Self Assessment Question.

Self Assessment Question 3

(a) What are the major security challenges in cyberspace?
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................

(b) What are the forms of data related threat in cyberspace?
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................
........................................................................................................................................

5.6 THE CONCEPT OF CYBER SECURITY

As discussed above, securing cyberspace and ensuring adequate legal and technological protection is a collaborative effort between users (including nations) and technology. Technological innovations focussed at minimizing cyber crimes, should be backed by substantial legislations. Hence, cyber security rests on two pillars; (i) technological innovations and its applications by end users; and (ii) legislations against cyber crimes. Many are of the opinion that technology alone will be sufficient to secure cyberspace, but in the arena of social engineering, where any criminal act, or even its attempt, requires to be legally addressed for social stability, having strict legislations in place against cyber interference is absolutely essential.

5.6.1 Technology’s Answers to Cyber Security

The technology market today is booming with all types of security tools, software, hardware locks, etc. Innovation is positive. But is technology alone sufficient to secure cyberspace, without co-operation amongst its users? The answer is no. As discussed earlier, the internet is based on an end-to-end technology. So maximum control and observation may be applied at the two ends with a fair amount of control and observation in the medium. There are four types of technologies that may be applied for cyber security. When I speak of technologies I am not referring to tools.

i) Unilateral Technology

Unilateral technologies are technologies that each user can decide upon for themselves. Therefore, neither coordination nor negotiation is needed concerning their use. Important unilateral technologies for multilateral security are:

- Tools to help even inexperienced users to formulate all their protection goals, if necessary for each and every application or even each and every action;
The Concept of Security in Cyberspace

- (Portable) devices which are secure for their users in order to bootstrap security. The devices need minimal physical protection comprising direct input/output with their users and, if they are multipurpose, an operating system providing fine-grained access control and administration of rights for applications, adhering to the principle of least privilege. This is essential to limit the spread of Trojan horses, and can prevent computer viruses completely;
- Encryption of local storage media to conceal and/or authenticate its contents;
- Hiding of secret data in local multimedia contents or in the local file system using steganographic techniques, not only to conceal the contents of the secret data, but also its very existence;
- Watermarking or fingerprinting digital data using steganographic techniques to help prove authorship or copyright infringements; and
- Using only software whose source code is published and well checked or the security of which is certified by a trustworthy third party having access to the complete source code and all tools used for code generation. The best technique is to combine both approaches with regard to as much of the software as possible. It is only by using at least one of these two approaches that you can be reasonably certain that the software you use does not contain Trojan horses. More or less the same applies to hardware where all sources and tools used for design and production are needed as well to check for the absence of Trojan horses.

ii) **Bilateral Technologies**

Bilateral technologies can only be used if the communication partners cooperate. This means that some coordination and negotiation is needed concerning their use. Bilateral technologies include tools for negotiating security mechanisms and cryptographic and steganographic mechanisms for securing content.

Important bilateral technologies for multilateral security are:
- Tools to negotiate bilateral protection goals and security mechanisms.
- Cryptographic mechanisms and steganography mechanisms to secure the communication content.

iii) **Trilateral Technologies**

Trilateral technologies can only be used if a third party is involved to fulfill a specific task for the other participating parties. This means that more coordination and negotiation is needed concerning their use compared with unilateral – and in most cases as well, bilateral – technologies. Important trilateral technologies for multilateral security are:
- Tools to negotiate trilateral security mechanisms, e.g. for accountability;
- To provide an access infrastructure, whereby the users use certain access parameters while transmitting data. Users will have the liberty to change the access tools to prevent data interception;
- Security gateways provided by third parties are gaining popularity. Security gateways are provided in the internet to facilitate limited access to participating users only. This is often used by users for exchange of confidential information at a pre-determined secured gateway; and
- Mechanisms to provide for digital pseudonyms, i.e. a suitable combination of anonymity and accountability. In particular, there are mechanisms to securely transfer signatures between different pseudonyms of the same party. This is called transferring signatures between pseudonyms.
When pseudonyms are used during accountable value exchange, there are a number of possibilities for the tasks of the integrated third party:

- Identification of the user in event of fraud (pseudonyms are certified and the certification authority knows real identities), i.e. privacy of pseudonymous parties cannot be guaranteed.
- Mandatory deposit of payment with an active trustee to prevent fraud in spite of completely anonymous pseudonyms, i.e. privacy of the pseudonymous parties can be guaranteed.

Trilateral security technologies include public key infrastructure techniques which can use certified public keys, security gateways, and digital pseudonyms.

### iv) Multilateral Technologies

Multilateral technologies can only be used if a large number of independent parties cooperate. This means that coordination and possibly negotiation are needed on a large scale. Important multilateral technologies for multilateral security are:

- Tools to negotiate multilateral protection goals and security mechanisms, e.g. for anonymity and unobservability.
- Mechanisms to provide anonymity, unobservability, and unlinkability with regard to communications, i.e. protect who communicates when to whom and from where to where.

### 5.6.2 Cybersecurity and Law

Most countries are still unaware of the potential threats of cyber crime and are still to come up with any guidelines, let alone legislations.

Every nation, as part of the legal framework promoting trust and confidence in cyberspace, should have basic criminal laws against activities that attack the confidentiality, integrity or availability of computer data and computer systems.

As seen above, there are numerous forms of cyber crimes, it may be impossible to draft legislations for each of them, however any form of illegal cyber interference may be broadly categorised under four heads and appropriate legislations may be drafted to address each of them. These are discussed below:

**Data interception:** It should be prohibited to intentionally intercept, without right, by technical means, non-public transmissions of computer data to, from or within a computer system. This crime constitutes an essential element of cyber-trust, for it protects the confidentiality of communications. For example, it makes it illegal to intercept the e-mail of another person. In some countries interception of telephonic is conversation (without prior legal sanction by way of a court order) is illegal, similarly the same laws may be extended to interception of electronic data also.

**Data interference:** It should be a crime to intentionally damage, delete, degrade, alter or suppress data in someone else’s computer without right. This provision would cover, for example, intentionally sending viruses that delete files, or hacking a computer and changing or deleting data, or hacking a web site and changing its appearance. The element of intentionality is important, since otherwise producing defective software or unintentionally forwarding a virus would be a crime.

**System interference:** It should be a crime to intentionally cause serious hindrance without right to the functioning of a computer system by inputting, transmitting,
The Concept of Security in Cyberspace

damaging, deleting, deteriorating, altering or suppressing computer data. This provision should cover things like Denial of Service Attacks or introducing viruses into a system in ways that interfere with its normal usage. It is important that this offence include, as an element of the offense, the concept that there must be significant harm (e.g., a certain threshold of monetary loss) in order for an offense to occur; otherwise, ordinary online behaviour, such as sending one or just a few unsolicited e-mails, would be a crime, which is not sensible.

Illegal access: This is the crime of intentionally accessing, other’s computer systems without having rights. It can be thought of as the cyberspace equivalent of trespassing. (Looked at another way, illegal access is an offence against the confidentiality of stored data and therefore is analogous to illegal interception, which is an offence against the confidentiality of data in transit.) This crime must be carefully defined, lest it include common, harmless activity. In the most serious cases, the act of illegal access is part of another crime covered by the three listed above, such as data interference, or it involves another crime covered by offline law, such as theft of proprietary data (see below). In some legal systems, the definition of the crime of illegal access is limited to situations in which confidential information (medical or financial information) is taken, copied or viewed or where there is intent to obtain confidential information or where access is obtained only by defeating security measures.

Please answer the following Self Assessment Question.

<table>
<thead>
<tr>
<th>Self Assessment Question 4</th>
<th>Spend 3 Min.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the four main broad heads for classifying illegal cyber interference?</td>
<td></td>
</tr>
</tbody>
</table>

5.7 COMPUTER RELATED OR COMPUTER FACILITATED CRIME

Discussions of computer crime often extend into matters that are not crimes against computers, but are crimes facilitated by the use of computers. For example, theft is a crime in every legal system, and the criminal law should cover theft whether it occurs online or offline. Similarly, fraud is a crime, and ordinary fraud statutes will often use terminology that applies equally well to online conduct as it did to offline conduct. Other crimes, such as infringement of intellectual property rights or dissemination of child pornography also are not properly computer crimes—they are crimes that may be facilitated by the use of a computer. Most computer related crimes may be covered under existing criminal law provisions by carefully examining existing provisions.
5.8 APPLICATION OF BASIC CRIMINAL LAW CONCEPTS

Common concepts of the criminal law such as “aiding and abetting” or “attempt” may be also applied to Cybercrime. For example, launching a virus with intent to disrupt service might be a crime under the concept of intent even if the virus didn’t work as intended. Similarly, if a nation’s law has the concept of aiding and abetting, that might be applied to cyber-crime, such that one who intentionally produces a virus and provides it to another knowing or intending that it will be used to destroy data or interfere with a system may be guilty of data or network interference caused by the virus even if the virus was introduced into a network by someone else.

Let us now summarize the point covered in this unit.

5.9 SUMMARY

- ‘Cyberspace’ refers to objects and identities that exist — largely within the computing network and is different from the term ‘internet’.
- There are serious threats associated with cyberspace on account of the technology – packet – switching protocols, the end-to-end network design and the impossibility of centralized control.
- There is an urgent widespread requirement to protect and secure cyberspace on account of it being a target of creative misuse.
- Some of the common cyber related violations or crimes are as follows:
  (i) Hacking
  (ii) Child pornography
  (iii) Cyber stalking
  (iv) Denial of service
  (v) Malware
  (vi) Phishing
  (vii) Information warfare
  (viii) Data related violations
  (ix) Network related violations
- Cyber Security rests upon the two pillars of (a) technological innovations, and its applications by end users; and (b) legislations against cyber crimes.
- Technology’s answers to cyber security include unilateral, bilateral, trilateral and multilateral technologies.
- Illegal cyber interference may be on account of (a) data interception (b) data interference (c) system interference and (d) illegal access.
- Common concepts of criminal law are applicable to cyber crime.

5.10 TERMINAL QUESTIONS

1. What are the reasons that Cyberspace may be viewed as being insecure?
2. In simple terms describe the following cyber threats:
3. What are the kinds of data related and network related cyber threats? Describe in brief.

4. What are the various technological methodologies to counter cyber threats? Describe in brief.

5. What are the legal principles that can be used to counter cyber threats? Explain with examples.

5.11 ANSWERS AND HINTS

Self Assessment Questions

1. The three main reasons contributing to a lack of security in cyberspace are (a) technology packet switching protocols (b) end to end network design and (c) impossibility of centralized control.

2. The major losses that businesses face on account of insecurity in cyberspace are the loss of proprietary data, intellectual property and online access to customers, suppliers and international service interruptions.

3. (a) The major security challenges in cyberspace are:
   - Hacking
   - Child pornography
   - Cyber Stalking
   - Denial of service
   - Malware
   - Phishing
   - Information warfare
   - Data related challenges and
   - Network related challenges

   (b) The three major forms of data related threat in cyberspace are:
       (a) Data interception
       (b) Data modification
       (c) Data theft

4. The four major heads for categorising illegal cyber interference are:
   (a) Data interception
   (b) Data interference
   (c) System interference and
   (d) Illegal access
Data Security

Terminal Questions
1. Refer to section 5.3 of the unit.
2. Refer to section 5.5 of the unit.
3. Refer to section 5.5 of the unit.
4. Refer to section 5.6 of the unit.
5. Refer to section 5.6 and 5.8 of the unit.

5.12 REFERENCES AND SUGGESTED READINGS


