Cyber Security and Ethical Hacking

UNIT-1: Introduction to Cybercrime

1. Introduction

2. Cybercrime: Definition and Origins of the Word

3. Cybercrime and Information Security

4. Who are Cybercriminals?

5. Classifications of Cyber Crimes

6. Cybercrime: The Legal Perspectives

7. Cybercrimes: An Indian Perspective

8. Cybercrime and the Indian ITA 2000

9. A Global Perspective on Cyber Crimes

1. Introduction

"Cyber security: is the protection of internet-connected systems, including hardware, software and data, from cyber attacks".

"Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. Almost everyone is aware of the rapid growth of the Internet. Given the unrestricted number of free websites, the Internet has opened a new way of exploitation known as cyber crime. These activities involve the use of computers, the Internet, cyberspace and the worldwide web (www. Cybercrime is not a new phenomena; the first recorded cyber crime 1820. It is one of the most talked about topics in the recent year.
Figure 1.1, based on a 2008 survey in Australia, shows the cybercrime trend.

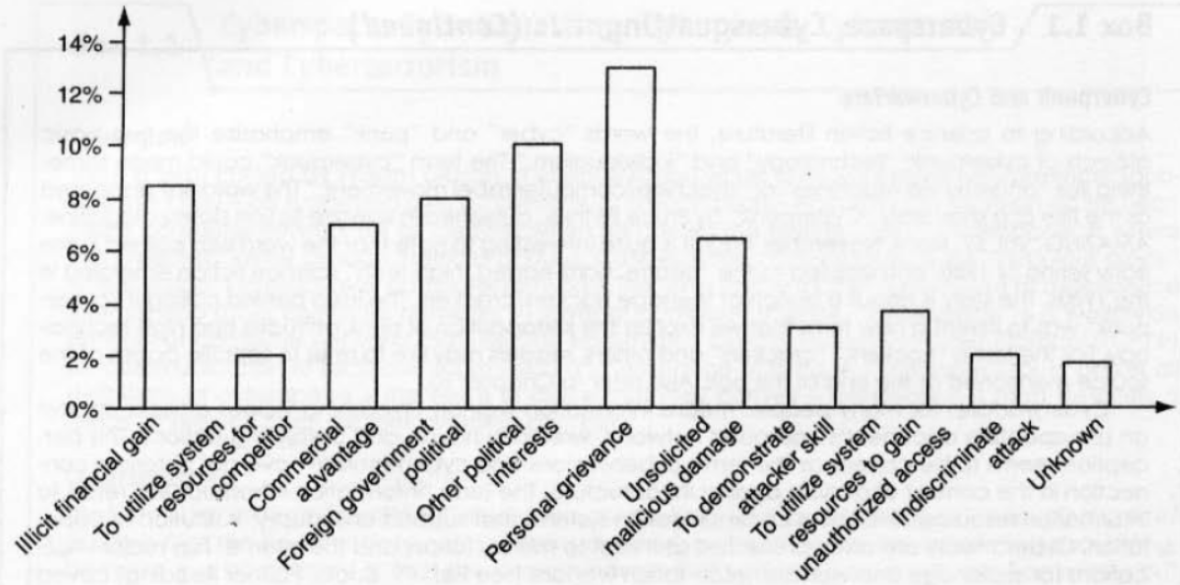

Figure 1.1 Cybercrime trend.
Source: 2008 Pacific Islands Computer Crime and Security Survey. Adapted from *Cybercrime: Threats, Challenges* presentation by Wipul Jayawickrama at the Computer Security Week 2008 in Brisbane, Australia (reproduced with permission).

- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.

- There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months-between January and June 2009.
- Various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTS).

2. **Cybercrime: Definition and Origins of the Word**

Cybercrime: "a crime conducted in which a computer was directly and significantly instrumental."

Alternative definitions of Cybercrime are as follows:

1. **Any illegal act** where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.

2. **Any traditional crime** that has acquired a new dimension or order of magnitude, through the aid of a computer, and abuses that have come into being because of computers

3. Any **financial dishonesty** that takes place in a computer environment.

4. Any **threats to the computer** itself, such as theft of hardware or software, damage and demands for money.

5. "Cyber crime (computer crime) is any **illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them**.

Note that in a wider sense, "computer-related crime" can be any illegal behavior committed by means of, or in relation to, a computer system or network; however, this is not cybercrime.

The term "cybercrime" relates to a number of other terms that may sometimes be used to describe crimes committed using computers.

- Computer-related crime
- Computer crime
- Internet crime
- E-crime
- High-tech crime, etc. are the other synonyms terms

Cybercrime specifically can be **defined** in a number of ways; a few definitions are:
1. A crime commited using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
2. Crimes completed either on os with a computer.
3. Any illegal activity done through the Internet or on the computer.
4. All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW

- According to one information security, cybercrime is any criminal activity which uses network access to commit a criminal act
- Cybercrime may be internal or external, with the former easier to perpetrate.
- The term "cybercrime" has evolved over the past few years since the adoption of Internet connection on a global scale with hundreds of millions of users.
- Cybercrime refers to the act of performing a criminal act using cyberspace as the communications vehicle.

The legal systems around the world introduce laws to combat cyber criminals attacks.
Two types of attack are as follows.

1. **Techno-crime**: An act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system.

2. **Techno-vandalism**: These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. "Tight internal security" and "strong technical safeguards" should prevent the vast majority of such incidents.

There is a very thin line between the two terms "computer crime" and "computer fraud both are punishable.

Cybercrimes (harmful acts committed from or against a computer or network) differ from most crimes in four ways:

(a) how to commit them is easier to learn,
(b) they require few resources relative to the potential damage caused
(c) they can be committed in a jurisdiction without being physically present in it
(d) they are often not clearly illegal

Important Definitions related to Cyber Security

a. *Cyber terrorism*

Cyber terrorism is defined as person or a group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyber terrorism."

- Cybercrime, especially through the Internet, has grown in number as the use of computers has become central to commerce, entertainment and government.
- The term cyber has some interesting synonyms: fake, replicated, pretend, imitation, virtual, computer generated.
- Cyber means combining forms relating to Information Technology, the Internet and Virtual Reality

b. *Cybernetics*

- This term owes its origin to the word "cybernetics" which deals with information and its use;
- Cybernetics is the science that overlaps the fields of neurophysiology, information theory. computing machinery and automation.
- Worldwide, including India, cyber terrorists usually use computers as a tool, a target for their unlawful act to gain information.
- The Internet is one of the means by which the offenders can gain priced sensitive information of companies, firms, individuals, banks and can lead to intellectual property (IP) crimes, selling illegal articles, pornography/child pornography, etc.

- This is done using methods such as Phishing, Spoofing, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual.

c. *Phishing*

It refers to an attack using mail programs to deceive or coax (lure) Internet users into disclosing confidential information that can be then exploited for illegal purposes. Figure 1.2 shows the increase in Phishing hosts.

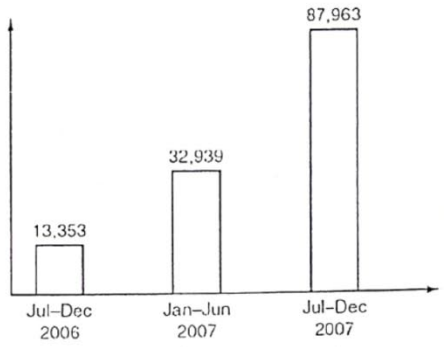

Figure 1.2 | Rise in the number of Phishing hosts.
Source: Symantec (International Telecommunications Society, 17th Biennial Conference, Montreal, Canada, June 24–27, 2008).

d. *Cyberspace*

- "cyberspace" is where users mentally travel through matrices of data. Conceptually, "cyberspace" is the nebulous place where humans interact over computer networks.
- The term "cyberspace" is now used to describe the Internet and other computer networks.
- In terms of computer science, "cyberspace" is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data.
- Cyberspace is most definitely a place where you chat, explore, research and play.

e. *Cyber squatting*

- The term is derived from "squatting" which is the act of occupying an abandoned space/ building that the user does not own, rent or otherwise have permission to use.
- Cyber squatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cyber squatters through the registration process.
- Cyber squatters usually ask for prices far greater than those at which they purchased it. Some cyber squatters put up derogatory or defamatory remarks about the person or

company the domain is meant to represent in an effort to encourage the subject to buy the domain from them.

- This term is explained here because, in a way, it relates to cybercrime given the intent of cyber squatting.
- Cyber squatting means registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. In this nature, it can be considered to be a type of cybercrime.
- Cyber squatting is the practice of buying "domain names" that have existing business names.

f. *Cyberpunk*

- According to science fiction literature, the words "cyber" and "punk emphasize the two basic aspects of cyberpunk: "technology" and "individualism."
- The term "cyberpunk" could mean something like "anarchy via machines" or ``machine/computer rebel movement."

g. *Cyberwarfare*

- Cyberwarfare means information attacks against an unsuspecting opponent's computer networks, destroying paralyzing nations.
- This perception seems to be correct as the terms cyber warfare and cyber terrorism have got historical connection in the context of attacks against infrastructure. The term "information infrastructure" refers to information resources, including communication systems that support an industry, institution or population.
- These types of Cyber attacks are often presented as a threat to military forces and the Internet has major implications for espionage and warfare.

3. **Cybercrime and Information Security**

- Lack of information security gives rise to cybercrimes.
- Let us refer to the amended indian Information Technology Act (ITA) 2000 in the context of cybercrime. From an Indian perspective, the new version of the Act (referred to as ITA 2008) provides a new focus on Information Security in India."
- Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access. use, disclosure, disruption, modification or destruction.
- The term incorporates both the physical security of devices as well as the information stored therein.
- It covers protection from unauthorized access, use, disclosure, disruption, modification and destruction.
- Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft.
- The 2008 CSI Survey on computer crime and security supports this.

- Cybercrimes occupy an important space in the information security domain because of their impact.
- The other challenge comes from the difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data gets stolen/lost (through loss/theft of laptops).
- Because of these reasons, reporting of financial losses often remains approximate.
- In an attempt to avoid negative publicity, most organizations abstain from revealing facts and figures about "security incidents" including cybercrime.
- In general, organizations' perception about "insider attacks" seems to be different than that made out by security solution vendors.
- However, this perception of an organization does not seem to be true as revealed by the 2008 CSI Survey. Awareness about "data privacy" too tends to be low in most organizations.
- When we speak of financial losses to the organization and significant insider crimes, such as leaking customer data, such "crimes" may not be detected by the victimized organization and no direct costs may be associated with the theft.

Table 1.5

Table 1.5 | Cybercrime trend over the years (1999–2008)

Types of Cybercrime	*2004 (%)*	*2005 (%)*	*2006 (%)*	*2007 (%)*	*2008 (%)*
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42	59	44
System penetration	17	14	15	13	13
Sabotage	5	2	3	4	2
Theft/loss of proprietary information	10	9	9	8	9
• from mobile devices					4
• from all other sources					5
Website defacement (see Figs. 1.6–1.10)	7	5	6	10	6
Abuse of wireless network	15	16	14	17	14
Misuse of web application	10	5	6	9	11
Bots (see Box 1.2; more in Chapter 2)				21	20
DoS attacks				6	8
Instant messaging abuse				25	21

Cybercrime trend over the years (1099-2008)

Figure 1.4 shows several categories of incidences - viruses, insider abuse, laptop theft and unauthorized access to systems.

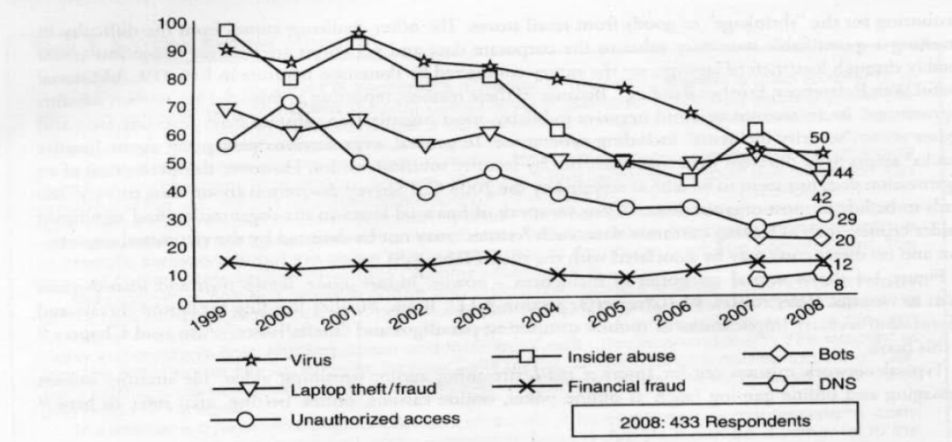

Figure 1.4 Major types of incidents by percentage.
Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

Typical network misuses :

- Internet radio/streaming audio,
- streaming video
- file sharing
- instant messaging
- online gaming
- Online gambling is illegal in some countries - for example, in India.

4. **Who are Cybercriminals?**

Cybercrime involves such activities

- credit card fraud
- cyberstalking
- defaming another online
- gaining unauthorized access to computer systems
- Ignoring copyright, software licensing and trademark protection Overriding encryption to make illegal copies
- Software piracy and stealing another's identity (known as identity perform criminal acts Cybercriminals are those who conduct such acts.

Types of Cybercriminals

1. Type I: Cybercriminals-hungry for recognition

- Hobby hackers
- IT professionals (social engineering is one of the biggest threat)
- Politically motivated hackers:
- Terrorist organizations.

2. Type II: Cybercriminals-

- Psychological perverts
- Financially motivated hackers (corporate espionage)

3. Type III: Cybercriminals the insiders

- Disgruntled or former employees seeking revenge
- Competing companies using employees to gain economic advantage through damage and/or theft.

5. **Classifications of Cybercrimes**

Cybercrimes are classified as follows:

5.1 Cybercrime against individual

a. Electronic mail (E-Mail) Spoofing and other online frauds:

- A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source.
- For example, let us say, Roopa has an E-Mail address roopa@asianlivs or Let us say her boyfriend Suresh and she happen to have a show down Then Suresh having become her enemy, spoofs her E-Mail and sends vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from Roopa her friends could take offense and relationships could be spoiled for life.

b. Online Frauds

- Online Scams. There are a few major types of crimes under the category of hacking
- Spoofing website and E-Mail security alert false mails about virus threats, lottery frauds and Spoofing.
- In Spoofing websites and E-Mail Security-threats, fraudsters create authentic looking websites that are actually nothing but a spoof.
- The purpose of these websites is to make the user enter personal information which is then used to access business and bank accounts.
- Fraudsters are increasingly turning to E-Mail to generate traffic to these websites.
- This kind of online fraud is common in the banking and financial sector.
- There is a rise in the number of financial institutions' customers who receive such E-Mails which usually contain link to a spoof website and mislead users to enter user ids and passwords. on the pretense that security details can be updated or passwords changed. It is wise he is alert and careful about E-Mails containing an embedded link, with a request for you to enter secret details. It is strongly recommended not to input any sensitive information that might help criminals to gain access to sensitive information, such as bank account details, even if the page appears legitimate.
- In virus E-Mails, the warnings may be genuine, so there is always a dilemma whether to take them lightly or seriously.
- A wise action is to first confirm by visiting an antivirus site such as McAfee, Sophos or Symantec before taking any action, such as forwarding them to friends and colleagues.

c. Phishing, Spear Phishing and its various other forms such as Vishing and Smishing

"**Phishing**" refers to an attack using mail programs to deceive or coax (lure) Internet users into disclosing confidential information that can be then exploited for illegal purposes.

"**Spear Phishing**" is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. Here

"**Vishing**" is the criminal practice of using social engineering over the telephone system. most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward:

- The term is a combination of V-voice and Phishing.
- Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.
- The most profitable uses of the information gained through a Vishing attack include:

1. ID theft
2. purchasing luxury goods and services
3. transferring money/funds
4. monitoring the victims' bank accounts
5. Making applications for loans and credit cards

"**Smishing**" is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from SMS PHISHING" SMS - Short Message Service is the text messages communication component dominantly used in mobile phones.

d. Spamming:

People who create electronic Spam are called spammers.
Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages indiscriminately.

1. Although the most widely recognized form of Spam is E-Mail Spam, the term is applied to similar abuses in other media: instant messaging Spam
2. Usenet newsgroup Spam
3. web search engine Spam
4. Spam in blogs
5. wiki Spam
6. online classified ads Spam
7. mobile phone messaging Spam
8. Internet forum Spam
9. junk fax transmissions, social networking Spam
10. file sharing network Spam
11. video sharing sites, etc.

- Spamming is difficult to control because it has economic viability - advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings.
- Spammers are numerous; the volume of unrequested mail has become very high because the barrier to entry is low.
- The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers (ISPs), who are forced to add extra capacity to cope with the deluge. Spamming is widely detested, and has been the subject of legislation in many jurisdictions - for example, the CAN-SPAM Act of 2003.
- Therefore, the following web publishing techniques should be avoided!

1. Repeating keywords;
2. use of keywords that do not relate to the content on the sig
3. use of fast meta refresh;
4. redirection;
5. IP Cloaking;
6. use of colored text on the same color background
7. tiny text usage;
8. duplication of pages with different URLS:
9. hidden links;
10. use of different pages that bridge to the same URL (gateway pages).

e. Cyber defamation:

- Cyber defamation is a Software offense.
- Let us first understand what the term entails. CHAPTER XXI of the Indian Penal Code (IPC) is about DEFAMATION. In Section 499 of CHAPTER XXI of IPC, regarding "defamation" there is a mention that

"*Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, exceppin The cases hereinafter expected, to defame that person.*"

- Cyber Defamation happens when the above takes place in an electronic form.
- In other words, cyberdefamation" occurs when defamation takes place with the help of computers and/or the Internet, for example, someone publishes a defamatory matter about someone on a website or sends an E-Mail containing defamatory information to all friends of that person. According to the IPC Section 499:

1. It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

f. Cyberstalking and harassment:

- The dictionary meaning of "stalking" is an "act or process of following prey stealthily - trying to approach somebody or something."
- Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.

g. Computer sabotage:

- The use of the Internet to stop the normal functioning of a computer system through the introduction of worms, viruses or logic bombs, is referred to as computer sabotage.
- It can be used to gain economic advantage over a competitor, to promote the illegal activities of terrorists or to steal data or programs for extortion purposes
- Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs.
- Some viruses may be termed as logic bombs because they tie dormant all through the year and become active only on a particular date.

h. Pornographic offenses:

- "Child pornography" means any visual depiction, including but not limited to the following:
- 1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer.
- 2. film, video, picture;
- 3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

- the Internet has become a household commodity in the urban areas of the nation. Its explosion has made the children a viable victim to the cybercrime.
- As the broad-band connections get into the reach of more and more homes, a larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of pedophiles.
- "Pedophiles" a person who is sexually attracted to children.

Here is how pedophiles operate:

- Step 1: Pedophiles use a false identity to trap the children/teenagers (using "false identity" which in itself is another crime called "identity theft").

- Step 2: They seek children/teens in the kids' areas on the services, such as the Games BB or chat areas where the children gather

- Step 3: They befriend children/teens

- Step 4: They extract personal information from the child/teen by winning his/her confidence.

- Step 5: Pedophiles get E-Mail address of the child/teen and start making contacts on the victim's E-Mail address as well. Sometimes, these E-Mails contain sexually explicit language.

- Step 6: They start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is created in the mind of the victim that what is being fed to him is normal and that everybody does it.

- Step 7: At the end of it, the pedophiles set up a meeting with the child/tech out of the house and then drag him/her into the not to further sexually assault him/her Br to use him/her as a sex object.

- This is the digital world"; in physical world, parents know the face of Dangers and they know how to avoid and face the problems by following simple rules and accordingly they advice their children to keep away from dangerous things and ways However, it is possible, even in the modem times most parents, may not know the basics of the Internet and the associated (hidden) dangers from the services offered over the Internet. Hence most children may remain unprotected in the cyberworld.

- Pedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is right/wrong for them while browsing the Internet.

- Legal remedies exist only to some extent
- for example, Children's Online Privacy Protection Act or COPPA is a way of preventing online pornography.

i. Password sniffing:

This also belongs to the category of cybercrimes against organization because the use of password could be by an individual for his/her personal work or the work he/she is doing using a computer that belongs to an organization.

5.2. Cybercrime against property

a. Credit card frauds:

- Information security requirements for anyone handling credit cards have increased dramatically recently.
- Millions of dollars may be lost annually by consumers who have credit card and calling card numbers stolen from online databases.

- Security measures are improving, and traditional methods of law enforcement seem to be sufficient for prosecuting the thieves of such information. Bulletin boards and other online services are frequent targets for hackers who want to access large databases of credit card information.
- Such attacks usually result in the implementation of stronger security systems.
- Security of cardholder data has become one of the biggest issues facing the payment card industry.
- Payment Card Industry Data Security Standard (PCI-DSS) is a set of regulations developed jointly by the leading card schemes to prevent cardholder data theft and to help combat credit card fraud.

b. Intellectual property (IP) crimes:

Basically, IP crimes include

- software piracy,
- copyright infringement,
- trademarks violations,
- theft of computer source code, etc.

c. Internet time theft:

- Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person.
- Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking on by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. RGAN
- However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent.
- The issue of Internet time theft is related to the crimes conducted through "identity theft."

5.3. Cybercrime against organization

a. Unauthorized accessing of computer Hacking is one method of doing this and hacking is a punishable offense

b. Password sniffing:

- Password Sniffers are programs that monitor and record the name and password of network users as they login jeopardizing security at a site.
- Whoever installs the Sniffer can then impersonate an authorized user and login to access restricted documents.
- Laws are not yet set up to adequately prosecute a person for impersonating another person online
- Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs.

c. Denial-of-service attacks (known as DoS attacks):

The goal of DoS is not to gain unauthorized access to systems or data, but to prevent intended users (i.e., legitimate users) of a service from using it. A DoS attack may do the following:

1. Flood a network with traffic, thereby preventing legitimate network traffic. systems, thereby preventing access to a service.
2. Disrupt connections between two
3. Prevent a particular individual from accessing a service.
4. Disrupt service to a specific system or person.

d. Virus attacks:

- Virus attacks can be used to damage the system to make the system unavailable
- Computer virus is a program that can "infect" legitimate (valid) programs by modifying them to include a possibly "evolved" copy of itself.
- Viruses spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines.
- A computer virus passes from computer to computer in a similar manner as a biological virus passed from person to person.
- Viruses may also contain malicious instructions that may cause damage at annoyance; the combination of possibly Malicious Code with the ability to spreadais viruses a considerable concern. Viruses can often spread without any readily visible symptoms.

e. E-Mail bombing/mail bombs:

- E-Mail bombing refers to sending a large number E-Mails to the victim to crash victim's E-Mail account (in the case of an individual) or to make victim's mail servers crash (in the case of a company or an E-Mail service provider).
- Computer programs can be written to instruct a computer to do such tasks on a repeated basis. In recent times, terrorism has hit the Internet in the form of mail bombings.
- By instructing a computer to repeatedly send E-Mail to a specific person's E-Mail address, the cybercriminal can overwhelm the recipient's personal account and potentially shut down entire systems. This may or may not be illegal, but it is certainly disruptive.

f. Salami attack/Salami Technique:

- These attacks are used for committing financial crimes.
- The idea here is to make the alloration so insignificant that in a single case it would go completely unnoticed; for example a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say '2/- or a few cents in a month) from the account of every customer.
- No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.

g. Logic bomb:

- Logic bombs are event-dependent programs created to do something only when a certain event (known as a trigger event) occurs.
- Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.

h. Trojan Horse:

- Trojan Horses: A Trojan Horse, Trojan for short, is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system

i. Data diddling:

- A data diddling (data cheating) attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.
- Electricity Boards in India have been victims to data diddling programs inserted when private parties computerize their systems.

j. Crimes emanating from Usenet newsgroup:

- As explained earlier, this is one form of spamming. The word "Spam" was usually taken to mean Excessive Multiple Posting (EMP).
- The advent of Google Groups, and its large Usenet archive, has made Usenet more attractive to spammers than ever.
- Spamming of Usenet newsgroups actually predates E-Mail Spam.
- Bot Serdar Argic also appeared in early 1994, posting tens of thousands of messages to various newsgroups, consisting of identical copies of a political screed relating to the Armenian Genocide.

k. Industrial spying/industrial espionage:

- Spying is not limited to governments. Corporations, like governments, often spy on the enemy.
- The Internet and privately networked systems provide new and better opportunities for espionage.
- "Spies" can get information about produce finances, research and development and marketing strategies, an activity known as "industrial spying."
- However, cyberspies rarely leave behind a trail
- Industrial spying is not newn fact it is as old as industries themselves. The use of the Internet to achieve this is probably as old as the Internet itself.
- Traditionally, this has been the reserved hunting field of a few hundreds of highly skilled hackers, contracted by high-profile companies or certain governments via the means of
- registered organizations (it is said that they get several hundreds of thousands of dollars, depending on the "assignment").
- With the growing public availability of Trojans and Spyware material, even low-skilled individuals are now inclined to generate high volume profit out of industrial spying. This is referred to as "Targeted Attacks" (which includes "Spear Phishing").

l. Computer network intrusions:

- Crackers" who are often misnamed "Hackers can break into computer systems from anywhere in the world and steal data, plant viruses, create backdoors, insert Trojan Horses or change user names and passwords.
- Network intrusions are illegal, but detection and enforcement are difficult.
- Current laws are limited and many intrusions go undetected.
- The cracker can bypass existing password protection by creating a program to capture login IDs and passwords.
- The practice of "strong password" is therefore important.

m. Software piracy:

- This is a big challenge area indeed.
- Cybercrime investigation cell of India defines "software piracy" as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.
- There are many examples of software piracy:

1. end-user copying friends loaning disks to each other, or organizations under- - reporting the number of software installations they have made, or organizations not tracking their software licenses;
2. hard disk loading with illicit means-hard disk vendors load pirated software;
3. counterfeiting - large-scale duplication and distribution of illegally copied software; illegal downloads from the Internet - by intrusion by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose:

(a) getting untested software that may have been copied thousands of times over,
(b) the software, if pirated, may potentially contain hard-drive-infecting viruses,
(c) there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users.
(d) there is no warranty projection, (e) there is no legal right to be the product, etc..

5.4. Cybercrime against Society

a. Forgery

- Counterfeit currency note postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and Scanners. of CSE
- Outside many colleges there are miscreants soliciting the sale of fake mark-sheets or even degree certificates.
- These are made using computers and High quality scanners and printers. In fact, this is becoming a booming business involving large monetary amount given to student gangs in exchange for these bogus but authentic looking certificates.

b. Cyberterrorism:

Cyberterrorism is defined as "any person, group or organization who, with terrorist intent, Utilizes accesses/or aids in accessing a computer or computer network or electronic system or

electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offense of cyberterrorism."

c. Web jacking:

- Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it).
- Thus, the first stage of this crime involves "password sniffing."
- The actual owner of the website does not have any more control over what appears on that website.

5.5. Crimes emanating from Usenet newsgroup:

- By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way. Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.
- Usenet is a popular means of sharing and distributing information on the Web with respect to specific topics or subjects.
- Usenet is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics.
- In principle, it is possible to prevent the distribution of specific newsgroups. In reality, however, there is no technical method available for controlling the contents of any newsgroup.
- It is merely subject to self-regulation and net etiquette.
- It is feasible to block specific newsgroups, however this cannot be considered as a definitive solution to illegal or harmful content.
- It is possible to put Usenet to the following criminal use:

1. Distribution/sale of pornographic material;
2. distribution/sale of pirated software packages:
3. distribution of hacking software;
4. sale of stolen credit card numbers.
5. sale of stolen data/stolen property

5.6. Other cybercrime forms

5.6.1 Hacking

- Although the purposes of hacking are many, the main ones are as follows:

1. Greed
2. power
3. publicity
4. revenge
5. adventure
6. desire to access forbidden information; destructive mindset.

- Every act, committed toward breaking into a computer and/or network is hacking and it is an offense,
- Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destroy and they get enjoyment out of such destruction.
- Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money.
- They extort money from some corporate giant threatening him to publish the stolen information that is critical in nature.
- Government websites are hot on hackers' target lists and attacks on Government websites receive wide press coverage.
- For example, according to the story posted on December 2009, the NASA site was hacked via SQL Injection
- Hackers, crackers and phrackers[11] are some of the oft-heard terms. The original meaning of the word "hack" meaning an elegant, witty or inspired way of doing almost anything originated at MIT.
- The meaning has now changed to become something associated with the breaking into or harming any kind of computer or telecommunications system.
- Some people claim that those who break into computer systems should ideally be called "crackers" and those targeting phones should be known as "phreaks"

5.6.2 Identity Theft

- Identity theft is a fraud involving another person's identity for an illicit purpose? This occurs when a criminal uses someone else's identity for his/her own illegal purposes.
- Phishing and identity theft are related offenses
- Examples include fraudulently obtaining credit, stealing inong from the victim's bank accounts, using the victim's credit card number

5.6.3 Spam in Cyberworld

Basically, "Spam" is the abuse of electronic messaging systems to send unsolicited bulk-messages indiscriminately.
Although the most widely recognized form of Spam is E-Mail Spam, this term is applied to similar abuses in other media:

1. instant messaging Spam,
2. Usenet newsgroup Spam,
3. instant messaging Spam,
4. Usenet newsgroup Spam,
5. web search engine Spam,
6. Spam in blogs,
7. wiki Spam,
8. online classified ads Spam,
9. mobile phone messaging Spam,
10. Internet forum Spam,
11. junk fax transmissions,
12. file sharing network Spam.

Spam is caused by flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it.
Often, this may result in the notorious DoS attack.
Commercial advertising often happens to be the cause of Spam. Such advertisements are often for products of dubious reputation and fraud schemes meant to ngke people believe they can get rich overnight!
Some Spam may also get generated through quadestegal services.
Spam hardly costs much to the sender; most of the costs are paid for by the recipient or the carriers rather than by the sender.
People who engage in the activity of electronic Spam are called spammers.
Two main types of Spam are worth mentioning:
"cancellable Usenet Spam" in which a single message is sent to several Usenet newsgroups and
"E-Mail Spam" which targets individual users with direct mail messages.
Often, spammers create E-Mail Spam lists by scanning Usenet postings, by stealing Internet mailing lists or searching the Web for addresses.
Typically, it costs money to users if they receive E-Mail Spam.
Any person with measured phone service can read or receive their mail.
Spam does not cost much to people.
Spam does, however, cost money to ISPs and to online service providers to transmit Spam. Unfortunately, subscribers end up paying these costs because the costs are transmitted directly to subscribers.

6. Cybercrime: The Legal Perspectives

Cybercrime poses a biggest challenge.
Computer Crime: As per "Criminal Justice Resource Manual (1979) computer-related crime was defined in the broader meaning as: "any illegal act for which knowledge of computer technology is essential for a successful prosecution".
International legal aspects of computer crimes were studied in 1983. In that study, computer crime was consequently defined as:
"encompasses any illegal act for which knowledge of computer technology is essential for its commit".
Cybercrime, in a way, is the outcome of "globalization," However, globalization does not mean globalized welfare at all
Globalized information systems accommodate an increasing number of transnational offenses.
The network context of cybercrime makes it one of the most globalized offenses of the present and the most modernized threats of the future.
This problem can be resolved in two ways. One is to divide information systems into segments bordered by state boundaries (cross-border flow of information).
The other is to incorporate the legal system into an integrated entity obliterating these state boundaries.
Apparently, the first way is unrealistic. Although all ancient empires including Rome, Greece and Mongolia became historical remnants, and giant empires are not prevalent in the current world, the partition of information systems cannot be an imagined practice.
In a globally connected world, information systems become the unique empire without tangible territory.

7. Cybercrimes: An Indian Perspective

India has the fourth highest number of Internet users in the world.
According to the statistics posted on the site (http://www.iamai.in/), there are 45 million Internet users in India, 37% of all Internet accesses happen from cybercafes and 57% of Indian Internet users are between 18 and 35 years.
The population of educated youth is high in India.
It is reported that compared to the year 2006, cybercrime under the Information Technology (IT) Act recorded a whopping 50% increase in the year 2007
A point to note is that the majority of offenders were under 30 years. The maximum cybercrime cases, about 46%, were related incidents of cyberpornography, followed by hacking. In over 60% of these cases, offenders were between 18 and 30 years, according to the "Crime in 2007" report of the National Crime Record Bureau (NCI).Box 1.6 shows the Indian Statistics on cybercrimes.

 The Indian Government is doing its best to control cybercrimes.

For example, Delhi Police have now trained 100 of its officers in handling cybercrime and placed them in its Economic Offences Wing. RGA

As at the time of writing this, the officers were trained for 6 weeks in computer hardware and software, computer networks comprising data communication networks, network protocols, wireless networks and network security.

Box 1.6 Cybercrimes: Indian Statistics

(A) Cybercrimes:
Cases of Various Categories under ITA 2000 217 cases were registered under Information Technology Act (ITA) during the year 2007 as compared to 142 cases during the previous year (2006), thereby reporting an increase of 52.8% in 2007 over 2006. 22.3% cases (49 out of 2172cases) were reported from Maharashtra followed by Karnataka (40), Kerala (38) and Andhra Pradesh and Rajasthan (16 each).

45.6% (99 cases) of the total 217 cases registered under ITA 2000 were related to obscene publication/transmission in electronic form, known as cyberpornography.

86 persons were arrested for committing such offenses during 2007.

There were 76 cases of hacking with computer system during the year wherein 48 persons were arrested

Out of the total (76) hacking cases, the cases relating to loss/damage of computer resource/utility under Section 66(1) of the IT Act were 39.5% (30 cases) whereas the cases related to hacking under Section 66(2) of IT Act were 60.5% (46 cases).

Maharashtra (19) and Kerala (4) registered maximum cases under Section 66(1) of the IT

Act out of total 30 such cases at the National level.

Out of the total 46 cases relating to hacking under Section 66(2), most of the cases (31) were reported from Karnataka followed by Kerala (7) and Andhra Pradesh (3) . 29.9% of the 154 persons arrested in cases relating to ITA 2000 were from Maharashtra (46) followed by Karnataka and Madhya Pradesh (16 each). The age-wise profile of persons arrested in cybercrime cases under ITA 2000 showed that 63.0% of the offenders were in the age group 18-30 years (97 out of 154) and 29.9% of the offenders were in the age group 30-45 years (46 out of 154).

Tamil Nadu reported two offenders whose ages were below 18 years.

India is said to be the "youth country" given the population age distribution. From the potential resources perspective, this is supposed to be a great advantage; assuming that these youths will get appropriate training to develop the required professional skills in them.

However, from cybercrime perspective, this youth aspect does not seem good as revealed by cybercrime statistics in India.

Crime head-wise and age-group-wise profile of the offenders arrested under ITA 2000 revealed that 55.8% (86 out of 154) of the offenders were arrested under "Obscene publication/transmission in electronic form" of which 70.9% (61 out of 86) were in the age group 18-30 years.

50% (24 out of 48) of the total persons arrested for "Hacking with Computer Systems" were in the age group of 18-30 years.

(B) Cybercrimes: Cases of Various Categories under IPC

(B) Cybercrimes: Cases of Various Categories under IPC Section

A total of 339 cases were registered under IPC Sections during the year 2007 as compared to 311 such cases during 2006, thereby reporting an increase of 9.0%. Madhya Pradesh reported maximum number of such cases, nearly 46.6% of total cases (158 out of 339) followed by Andhra Pradesh 15.6% (53 cases) and Chhattisgarh 15.3% (52 cases). Majority of the crimes out of total 339 cases registered under IPC fall under two categories, viz., Forgery (217) and Criminal Breach of Trust or Fraud (73). Although such offenses fall under the traditional IPC crimes, these cases had the cyberovertones wherein computer, Internet or its enabled services were present in the crime and hence they were categorized as Cybercrimes under IPC. The cyberforgery (217 cases) accounted for 0.33% out of the 65,326 cases reported under cheating. The cyberfrauds (73) accounted for 0.47% of the total Criminal Breach of Trust cases (15,531).

The cyberforgery cases were the highest in Madhya Pradesh (133) followed by Chhattisgarh (26) and Andhra Pradesh (22). The cases of cyberfraud were highest in Madhya Pradesh (20) followed by Punjab (17) and Andhra Pradesh (15). A total of 429 persons were arrested in the country for Cybercrimes under IPC during 2007. 61.5% offenders (264) of these were taken into custody for offenses under "Cyberforgery," 19.8% (85) for "Criminal Breach of Trust/Fraud" and 11.4% (49) for "Counterfeiting Currency/Stamps."

States such as Madhya Pradesh (166), Anahra Pradesh (83), Chhattisgarh (82) and Punjab (69) have reported higher arrests for cybercrimes registered under IPC. The age-group-wise profile of the arrested persons showed that 55.2% (237 of 429) were in the age group of 30–45 years and 29.4% (126 of 429) of the offenders were in the age group of 18–30 years. Only four offenders from Chhattisgarh were below 18 years of age. Crime head-wise and age-wise profile of the offenders arrested under Cybercrimes (IPC) offenders involved in forgery cases were more in the age group of 30–45 (54.9%, 145

(C) Incidence of Cybercrimes in Cities

(C) Incidence of Cybercrimes in Cities

17 out of 35 mega cities did not report any case of cybercrime (neither under the IT Act nor under IPC Sections) during the year 2007. A total of 17 mega cities have reported 118 cases under IT Act and 7 mega cities reported 180 cases under various sections of IPC. There was an increase of 32.6% (from 89 cases in 2006 to 118 cases in 2007) in cases under IT Act as compared to previous year (2006), and an increase of 26.8% (from 142 cases in 2006 to 180 cases in 2007) of cases registered under various sections of IPC. Bengaluru (40), Pune (14) and Delhi (10) have reported high incidence of cases (64 out of 118 cases) registered under IT Act, accounting for more than half of the cases (54.2%) reported under the Act. Bhopal has reported the highest incidence (158 out of 180 cases) of cases reported under IPC sections accounting for 87.8%.

8. **Cybercrime and the Indian ITA 2000**

- In India, the ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/S1/162 on January 30, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.
- This was the first step toward the Law relating to E-Commerce at international level to regulate an alternative form of commerce and to give legal status in the area of E-Commerce.
- It was enacted taking into consideration UNICITRAL model of Law on Electronic Commerce (1996).

8.1 Hacking and the Indian Law(s)

- Cybercrimes are punishable under two categories: the ITA 2000 and the IPC

- A total of 207 cases of cybercrime were registered under the IT Act in 2007.compared to 142 cases registered in 2006. Under the: IPC too, 339 cases were recorded in 200% compared to 311 cases in 2006.
- There are some noteworthy provisions under the ITA 2000, which is said to be undergoing key changes very soon.

Hacking and the ITA 2008

- The number of Offenses to be monitored has increased. According to cyber law experts, "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime."
- Cases of Spam, hacking, cyberstalking and E-Mail fraud are rampant and, although cybercrimes cells have been set up in major cities, the problem is that most cases remain unreported due to a lack of awareness
- In an environment like this, there are a number of questions in the minds of a commoner:

1. When can consumers approach a cybercrime cell?
2. What should the victims do?
3. How does one maintain security online?
4. Any and every incident of cybercrime involving a computer or electronic network can be reported to a police station, irrespective of whether it maintains a separate cell or not.

- CHAPTER XI of the original ITA 2000 lists a number of activities that may be taken to constitute cybercrimes.
- This includes tampering with computer source code, hacking, publishing or transmitting any information in electronic form that is lascivious, securing access to a protected system, and Breach of confidentiality and privacy. In the original ITA 2000, the following is stated under CHAPTER XI (Offences):

1. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.
2. Whoever commits hacking shall be punished with imprisonment up to 3 years, or with fine which may extend up to 2 lakhs (200,000), or with both.

- In the amendment to the IT Act 2000, now known as the ITA 2008, several offenses have been added to the Act.
- The amendments have now revealed a whole bundle of surprises which will make the cybercrime police jump. Existing Sections 66 and 67 (in the original ITA 2000) on hacking and obscene material have been updated by dividing them into more crime-specific subsections, thereby making cybercrimes punishable.
- In Section 66, hacking as a term has been removed. This section has now been expanded to include Sections

1. 66A (offensive messages),
2. 66B (receiving stolen computer), o 66C (identity theft),
3. 66D (impersonation),
4. 66E (voyeurism) and

5. 66F (cyberterrorism). Section 66F is a new section of the IT 2008 recent amendments to the Indian ITA 2000). It covers "Cyberterrorisms and makes it punishable with imprisonment up to life term. This may cover hacking,
6. DoS attacks, Port Scanning, spreading viruses, etc., if it can be linked to the object of terrorizing people.

9. A Global Perspective on Cybercrimes

- In Australia, cybercrime has a narrow statutory meaning as used in the CyberCrime Act 2001, which details offenses against computer data and systems.
- However, a broad meaning is given to cybercrime at an international level. In the Council of Europe's (CoE's) Cyber Crime Treaty, cybercrime is used as an umbrella term to refer to an array of criminal activity including
- offenses against computer data and Systems,
- computer-related offenses,
- content offenses and copyright offenses.
- This wide definition of cybercrime overlaps in part with general offense categories that need not be Information & Communication Technology (ICT)-dependent, such as white-collar crime and economic crime.
- Although this status is from the International Telecommunication Union (ITU) survey : conducted in 2005, we get an idea about the global perspective.
- ITU activities on countering Spam can be read by visiting the link www.itu.int/spam (8 May 2010).
- The Spam legislation scenario mentions "none" about India as far as E-Mail legislation in India is concerned.
- The legislation refers to India as a "loose" legislation, although there is a mention in Section 67 of Indian ITA 2000.
- About 30 countries have enacted some form of anti-Spam legislation.
- There are also technical solutions by ISPs and end-users.
- However, in spite of this, so far there has been no significant impact on the volume of Spam with spammers sending hundreds of millions of messages per day.
- The growing phenomenon is the use of Spam to support fraudulent and criminal activities - including attempts to capture financial information (e.g., account numbers and passwords) by masquerading messages as originating from trusted companies ("brand-spoofing" or "Phishing") – and as a vehicle to spread viruses and worms.
- On mobile networks, a peculiar problem is that of sending bulk unsolicited text messages aimed at generating traffic to premium-rate numbers. As there are no national "boundaries" to such crimes under the cybercrime realm, it requires international cooperation between those who seek to enforce anti-Spam laws.
- Thus, one can see that there is a lot to do toward building confidence and security in the use of ICTs and moving toward an international cooperation agenda. This is because in the 21st century, there is a growing dependency on ICTS that span the globe. There was a rapid growth in ICTs and dependencies that led to a shift in perception of cybersecurity threats in the mid-1990s.
- The linkage of cybersecurity and critical infrastructure protection has become a big issue as a number of countries have begun assessment of threats, vulnerabilities and started exploring mechanisms to redress them.

Recently, there have been a number of significant developments such as

1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime. The convention targets hackers, those spreading destructive computer viruses (refer to Chapter 4), those using the Internet for the sexual exploitation of children or the distribution of racist material, and terrorists attempting to attack infrastructure facilities or financial institutions. The Convention is in full accord with all the US constitutional protections, such as free speech and other civil liberties, and will require no change to the US laws.

2. In August 18, 2006, there was a news article published "ISPs Wary About 'Drastic Obligations on Web Site Blocking." European Union (EU) officials want to debar suspicious websites as part of a 6-point plan to boost jo antiterrorism activities. They want to block websites that incite terrorist action. Once again it is underlined that monitoring calls, Internet and E-Mail traffic for law enforcement purposes is a task vested in the government, which must reimburse carriers and providers for retaining the data.

3. CoE Cyber Crime Convention (1997-2001) was the first international treaty seeking to address Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.[19] More than 40 countries have ratified the Convention to date.

One wonders as to what is the role of the business/private sector in taking up measures to prevent cybercrime and toward responsibilities and roles related to the ownership of information and communication infrastructures. Effective security requires an in-depth understanding of the various aspects of information and communication networks. Therefore, the private sector's expertise should be increasingly involved in the development and implementation of a country's cybersecurity strategy.