1. INTRODUCTION TO CYBERCRIME

List of Topics:

- Introduction
- Cybercrime: Definition and Origins of the Word
- Cybercrime and Information Security
- Who are Cybercriminals?
- Classifications of Cybercrimes
- Cybercrime: The Legal Perspectives
- Cybercrimes: An Indian Perspective
- Cybercrime and the Indian ITA 2000
- A Global Perspective on Cybercrimes
- Cybercrime Era: Survival Mantra for the Netizens

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 undeniably opened a new way of exploitation known as cybercrime.
- These activities involve the use of computers, the Internet, cyberspace and the worldwide web (WWW).
- Interestingly, cybercrime is not a new phenomena; the first recorded cybercrime took place in the year 1820.
- It is one of the most talked about topics in the recent years.
- Based on a 2008 survey in Australia, the below shows the cybercrime trend

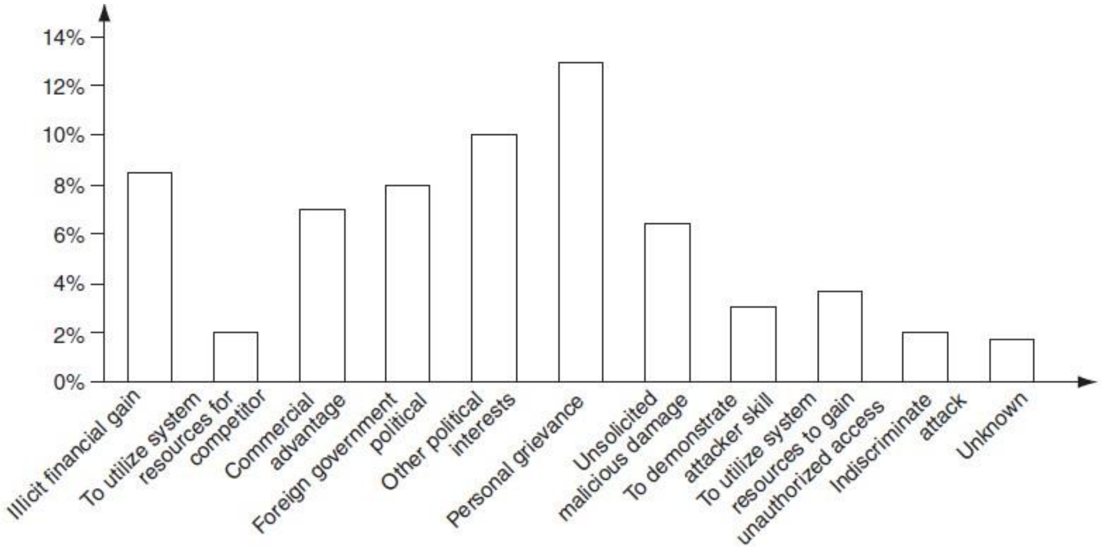


Figure: Cybercrime Trend

- 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).

CYBERCRIME: DEFINITION AND ORIGINS OF THE WORD

Definition:

“A crime conducted in which a computer was directly and significantly instrumental is called as a Cybercrime.”

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. "Cybercrime (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 synonymous terms.

Cybercrime specifically can be defined in a number of ways; a few definitions are:

1. A crime committed 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 or 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.

Some people argue that a cybercrime is not a crime as it is a crime against software & not against a person (or) property. However, while the legal systems around the world scramble to introduce laws to combat cyber criminals, 2 types of attacks are prevalent:

1. Techno-crime: A premeditated 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. The 24X7 connection to the internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, if any, "finger prints".
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, allied to 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 terrestrial 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:

Cyberterrorism:

This term was coined in 1997 by Barry Collin, a senior research fellow at the institute for Security and Intelligence in California. Cyberterrorism seems to be a controversial term. The use of information technology and means by terrorist groups & agents is called as Cyberterrorism.

“The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives.”

(or)

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 offence of cyberterrorism.”

Cybernetics:

Cybernetics 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, cyberterrorists usually use computer as a tool, target for their unlawful act to gain information.

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, Pharming, Internet Phishing, wire transfer, etc. and use it to their own advantage without the consent of the individual.

Phishing:

Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need a request from their bank, for instance, or a note from someone in their company and to click a link or download an attachment.

Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information from unsuspecting victims for identity theft, financial gain &amp; other fraudulent activities.

(or)

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords, credit card information from users etc.

Cyberspace:

This is a term coined by William Gibson, a science fiction writer in 1984. 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.

Cybersquatting:

The term is derived from "squatting" which is the act of occupying an abandoned/unoccupied space/ building that the user does not own, rent or otherwise have permission to use. Cybersquatting, however, is a bit different in that the domain names that are being squatted are (sometimes but not always) being paid for by the cybersquatters through the registration process.

Cybersquatters usually ask for prices far greater than those at which they purchased it. Some cybersquatters 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 cybersquatting.

Cybersquatting 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. Cybersquatting is the practice of buying "domain names" that have existing businesses names.

In India, Cybersquatting is considered to be an Intellectual Property Right (IPR). In India, Cybersquatting is seen to interfere with “Uniform Dispute Resolution Policy” (a contractual obligation to which all domain name registrants are presently subjected to).

Cyberpunk:

This is a term coined by Bruce Bethke, published in science fiction stories magazine in November 1983. 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.”

Cyberwarfare:

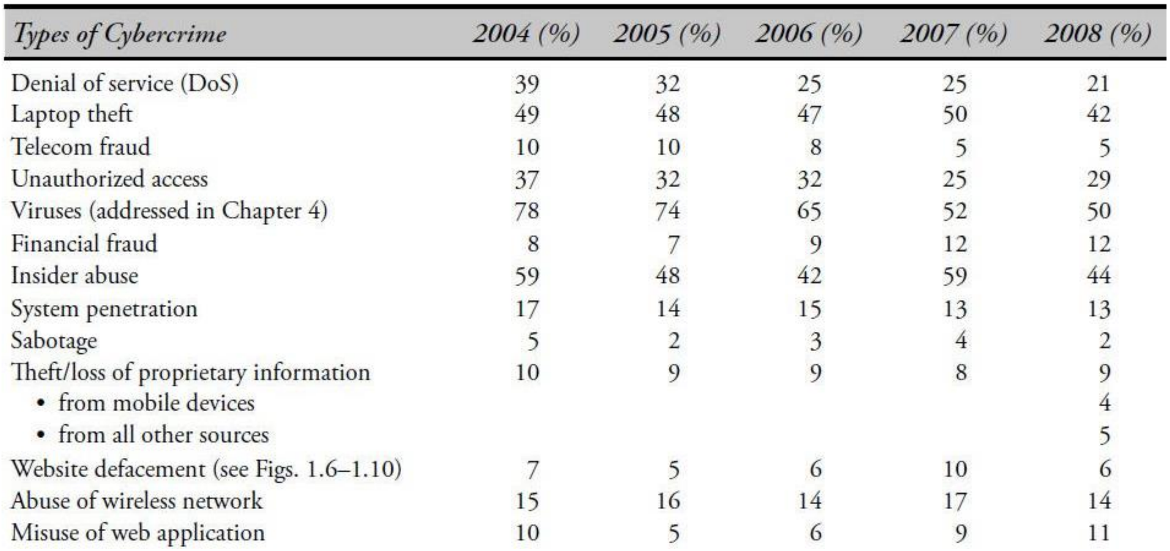
Cyberwarfare means information attacks against an unsuspecting opponent’s computer networks, destroying and paralyzing nations. This perception seems to be correct as the terms cyberwarfare and Cyberterrorism have got historical connection in the context of attacks against infrastructure. The term “information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

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.

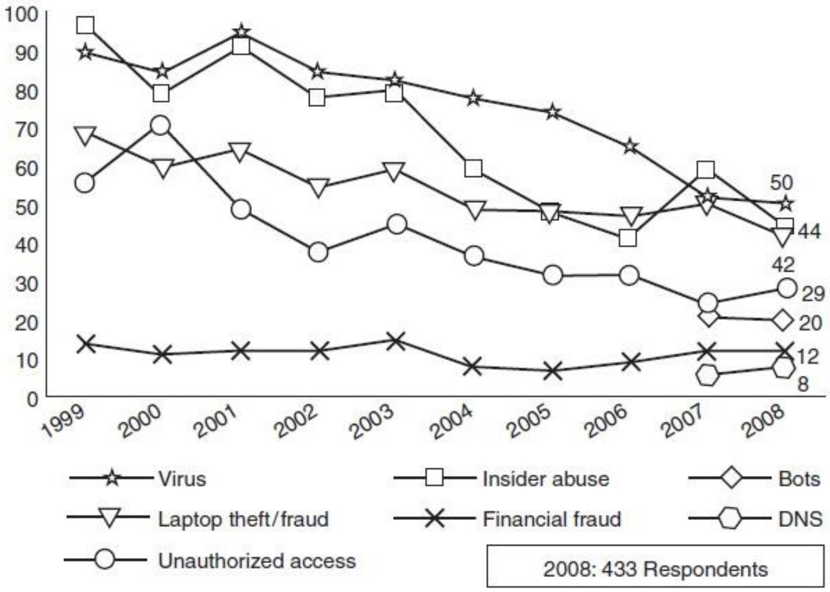
Where financial losses to the organization due to insider crimes are concerned (e.g., leaking customer data), often some difficulty is faced in estimating the losses because the financial impacts may not be detected by the victimized organization and no direct costs may be associated with the data theft. The 2008 CSI Survey on computer crime and security supports this. Cybercrimes occupy an important space in 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 get 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 vendor. 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



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

<u>Figure</u>: Cybercrime trend over the years



<u>Figure</u>: shows several categories of incidences – viruses, insider abuse, laptop theft and unauthorized access to systems

The Botnet Menace:

A group of computers that are controlled by software containing harmful programs, without their users' knowledge is called as **Botnet**. The term “Botnet” is used to refer to a group of compromised computers (zombie computers, i.e., personal computers secretly under the control of hackers) running malwares under a common command and control infrastructure. Below figure shows how a “zombie” works.

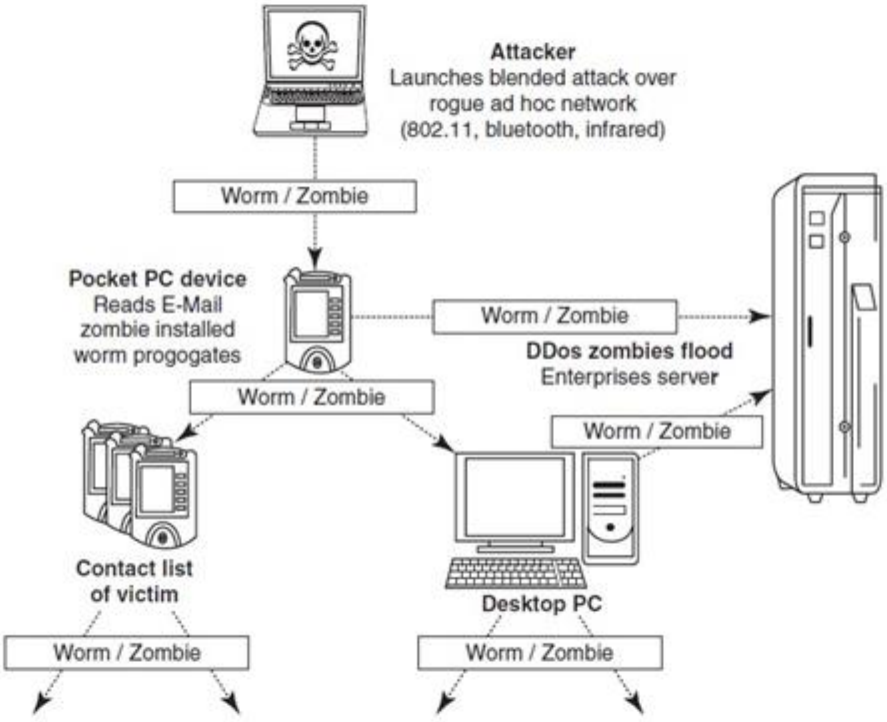


Figure: How a Zombie works

- A Botnet maker can control the group remotely for illegal purposes, the most common being
    - denial-of-service attack (DoS attack),
    - Adware,
    - Spyware,
    - E-Mail Spam,
    - Click Fraud
    - theft of application serial numbers,
    - login IDs
    - financial information such as credit card numbers, etc.
- An attacker usually gains control by infecting the computers with a virus or other Malicious Code. The computer may continue to operate normally without the owner’s knowledge that his computer has been compromised.
- The problem of Botnet is global in nature and India is also facing the same.

- India has an average of 374 new Bot attacks per day and had more than 38,000 distinct Bot-infected computers in the first half of the year 2009.
- Small and medium businesses in the country are at greater risk, as they are highly vulnerable to Bots, Phishing, Spam and Malicious Code attacks.
    - Mumbai with 33% incidences tops the Bot-infected city list,
    - followed by New Delhi at 25%,
    - Chennai at 17% and
    - Bangalore at 13%.
- Tier-II locations are now also a target of Bot-networks with Bhopal at 4% and Hyderabad, Surat, Pune and Noida at 1% each.
- The Internet is a network of interconnected computers. If the computers, computer systems, computer resources, etc. are unsecured and vulnerable to security threats, it can be detrimental to the critical infrastructure of the country.

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 theft) to perform criminal acts

<u>Types of Cybercriminals</u>:

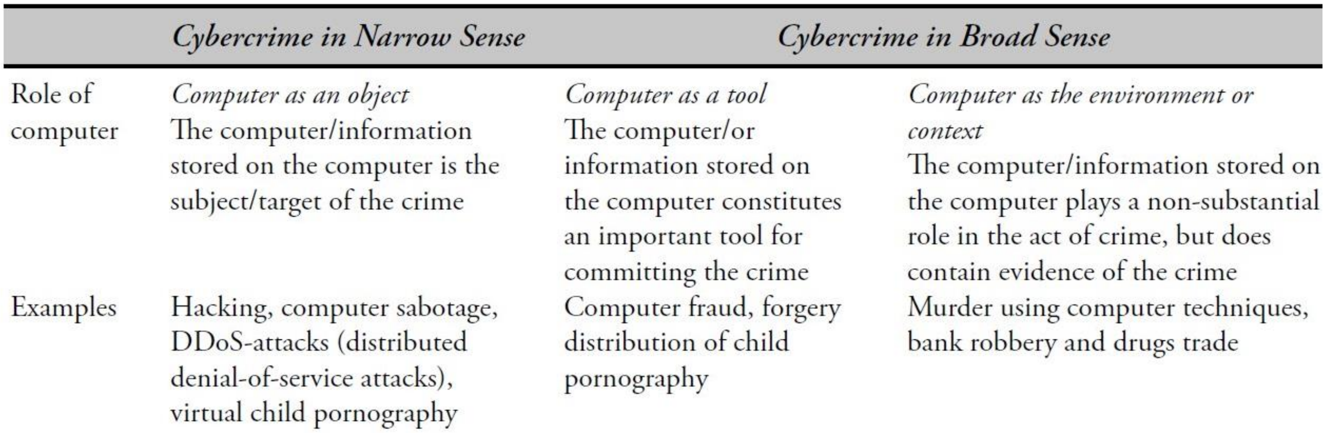
1. **Type I: Cybercriminals – hungry for recognition**
    - Hobby hackers;
    - IT professionals (social engineering is one of the biggest threat);
    - Politically motivated hackers;
    - Terrorist organizations.
2. **Type II: Cybercriminals – not interested in recognition**

- Psychological perverts;
- financially motivated hackers (corporate espionage);
- state-sponsored hacking (national espionage, sabotage)
- organized criminals

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.

CLASSIFICATIONS OF CYBERCRIMES



	Cybercrime in Narrow Sense	*Cybercrime in Broad Sense*	
Role of computer	*Computer as an object* The computer/information stored on the computer is the subject/target of the crime	*Computer as a tool* The computer/or information stored on the computer constitutes an important tool for committing the crime	*Computer as the environment or context* The computer/information stored on the computer plays a non-substantial role in the act of crime, but does contain evidence of the crime
Examples	Hacking, computer sabotage, DDoS-attacks (distributed denial-of-service attacks), virtual child pornography	Computer fraud, forgery distribution of child pornography	Murder using computer techniques, bank robbery and drugs trade

Table: Classifying Cybercrimes

"Crime is defined as an act or the commission of an act that is forbidden, or the omission of a duty that is commanded by a public law and that makes the off ender liable to punishment by that law". Cyber crimes are classified as follows:

- Cybercrime against individual
- Cybercrime against property
- Cybercrime against organization
- Cybercrime against society
- Crimes emanating from Usenet newsgroup

Cybercrime against individual

1. E-Mail Spoofing: 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@asianlaws.org. 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.

2. <u>Online Frauds</u>: The most common types of online fraud are called phishing and spoofing. Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc. Often times the e-mails directs you to a website where you can update your personal information. Because these sites often look “official,” they hope you’ll be tricked into disclosing valuable information that you normally would not reveal. This often times, results in identity theft and financial loss.

Spyware and viruses are both malicious programs that are loaded onto your computer without your knowledge. The purpose of these programs may be to capture or destroy information, to ruin computer performance or to overload you with advertising. Viruses can spread by infecting computers and then replicating. Spyware disguises itself as a legitimate application and embeds itself into your computer where it then monitors your activity and collects information.

3. <u>Phishing, Spear Phishing and its various other forms such as Vishing and Smishing</u>:

Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc. Often times the e-mails directs you to a website where you can update your personal information. Because these sites often look “official,” they hope you’ll be tricked into disclosing valuable information that you normally would not reveal. This often times, results in identity theft and financial loss.

Spear Phishing is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering. Here is how Spear Phishing scams work; Spear Phishing describes any highly targeted Phishing attack. Spear phishers send E-Mail that appears genuine to all the employees or members within a certain company, government agency, organization or group. The message might look as if it has come from your employer, or from a colleague who might send an E-Mail message to everyone in the company; it could include requests for usernames or passwords. While traditional Phishing scams are designed to steal information from individuals, spear phishing scam works to gain access to a company's entire computer system.

Vishing (voice phishing) is a type of phishing attack that is conducted by phone and often targets users of Voice over IP (VoIP) services like Skype.

It’s easy to for scammers to fake caller ID, so they can appear to be calling from a local area code or even from an organization you know. If you don’t pick up, then they’ll leave a voicemail message asking you to call back. Sometimes these kinds of scams will employ an answering service or even a call center that's unaware of the crime being perpetrated.

Once again, the aim is to get credit card details, birthdates, account sign-ins, or sometimes just to harvest phone numbers from your contacts. If you respond and call back, there may be an automated message prompting you to hand over data and many people won't question this, because they accept automated phone systems as part of daily life now.

Smishing (SMS phishing) is a type of phishing attack conducted using SMS (Short Message Services) on cell phones. Just like email phishing scams, smishing messages typically include a threat or enticement to click a link or call a number and hand over sensitive information. Sometimes they might suggest you install some security software, which turns out to be malware.

Smishing example: A typical smishing text message might say something along the lines of, "Your ABC Bank account has been suspended. To unlock your account, tap here: https://bit.ly/2LPLdaU" and the link provided will download malware onto your phone. Scammers are also adept at adjusting to the medium they're using, so you might get a text message that says, "Is this really a pic of you? https://bit.ly/2LPLdaU" and if you tap that link to find out, once again you're downloading malware.

4. 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. 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, Usenet newsgroup Spam, web search engine Spam, Spam in blogs, wiki Spam, online classified ads Spam, mobile phone messaging Spam, Internet forum Spam, junk fax transmissions, social networking Spam, file sharing network Spam, 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. Therefore, the following web publishing techniques should be avoided:

- Repeating keywords;
- use of keywords that do not relate to the content on the site;
- use of fast meta refresh;
- redirection;
- IP Cloaking;
- use of colored text on the same color background;
- tiny text usage;
- duplication of pages with different URLs;

- hidden links;
- use of different pages that bridge to the same URL (gateway pages).

5. <u>Cyber defamation</u>: It is a cognizable (Software) offense. **“**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, except in the cases hereinafter expected, to defame that person.**”**

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

6. <u>Cyberstalking and harassment</u>: 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.

As the internet has become an integral part of our personal & professional lives, cyberstalkers take advantage of ease of communication & an increased access to personal information available with a few mouse clicks or keystrokes. They are 2 types of stalkers: Online Stalkers: aim to start the interaction with the victim directly with the help of the internet. Offline Stalkers: the stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim.

7. <u>Computer Sabotage</u>: 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 lie dormant all through the year and become active only on a particular date.

8. <u>Pornographic Offenses</u>: 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.

Child Pornography is considered an offense. The internet is being highly used by its abusers to reach and abuse children sexually, worldwide. 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, larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of pedophiles. Pedophiles are the people who physically or psychologically coerce minors to engage in sexual activities, which the minors would not consciously consent too. Here is how pedophiles operate:

- Step 1: Pedophiles use a false identity to trap the children/teenagers.
- 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/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.

9. Password Sniffing: is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic.

And yet, password sniffers aren't always used for malicious intent. They are often used by IT professionals as a tool to identify weak applications that may be passing critical information unencrypted over the Local Area Network (LAN). IT practitioners know that users download and install risky software at times in their environment, running a passive password sniffer on the network of a business to identify leaky applications is one legitimate use of a password sniffer.

Cybercrime against property

1. **Credit Card Frauds:** Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help businesses process card payments securely and reduce

card fraud. Credit card fraud can be authorised, where the genuine customer themselves processes a payment to another account which is controlled by a criminal, or unauthorised, where the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party.

Credit cards are more secure than ever, with regulators, card providers and banks taking considerable time and effort to collaborate with investigators worldwide to ensure fraudsters aren't successful. Cardholders' money is usually protected from scammers with regulations that make the card provider and bank accountable. The technology and security measures behind credit cards are becoming increasingly sophisticated making it harder for fraudsters to steal money.

2. **Intellectual Property (IP) Crimes:** With the growth in the use of internet these days the cyber crimes are also growing. Cyber theft of Intellectual Property (IP) is one of them. Cyber theft of IP means stealing of copyrights, software piracy, trade secrets, patents etc., using internet and computers.

   Copyrights and trade secrets are the two forms of IP that is frequently stolen. For example, stealing of software, business strategies etc. Generally, the stolen material is sold to the rivals or others for further sale of the product. This may result in the huge loss to the company who originally created it. Another major cyber theft of IP faced by India is piracy. These days one can get pirated version of movies, software etc. The piracy results in a huge loss of revenue to the copyright holder. It is difficult to find the cyber thieves and punish them because everything they do is over internet, so they erase the data immediately and disappear within fraction of a second.

3. **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 or by gaining access to it by illegal means, uses it to access the Internet without the other person’s knowledge. 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.

Cybercrime against Organization

1. **Unauthorized accessing of Computer:** Hacking is one method of doing this and hacking is punishable offense. Unauthorized computer access, popularly referred to as hacking, describes a criminal action whereby someone uses a computer to knowingly gain access to data in a system without permission to access that data.
2. **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.

3. **Denial-of-service Attacks (DoS Attacks):** It is an attempt to make a computer resource (i.e.., information systems) unavailable to its intended users. In this type of criminal act, the attacker floods the bandwidth of the victim's network or fills his E-Mail box with spam mail depriving him of the services he is entitled to access or provide. 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:
   a. Flood a network with traffic, thereby preventing legitimate network traffic.
   b. Disrupt connections between two systems, thereby preventing access to a service.
   c. Prevent a particular individual from accessing a service.
   d. Disrupt service to a specific system or person.
4. **Virus attacks/dissemination of Viruses:**

   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 passes from person to person. Viruses may also contain malicious instructions that may cause damage or annoyance; the combination of possibly Malicious Code with the ability to spread is what makes viruses a considerable concern. Viruses can often spread without any readily visible symptoms. Viruses can take some typical actions:
   - Display a message to prompt an action which may set of the virus
   - Delete files inside the system into which viruses enter
   - Scramble data on a hard disk
   - Cause erratic screen behavior
   - Halt the system (PC)
   - Just replicate themselves to propagate further harm
5. **E-Mail bombing/Mail bombs:** E-Mail bombing refers to sending a large number of 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 program 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 specified 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.

6. **Salami Attack/Salami technique:** These attacks are used for committing financial crimes. The idea here is to make the alteration 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 Rs. 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.
7. **Logic Bomb:** A Logic Bomb is a piece of often-malicious code that is intentionally inserted into software. It is activated upon the host network only when certain conditions are met. Some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.
8. **Trojan Horse:** 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.
9. **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.
10. **Newsgroup Spam/Crimes emanating from Usenet newsgroup:** 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.
11. **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 product finances, research and development and marketing strategies, an activity known as "industrial spying."

    However, cyberspies rarely leave behind a trail. Industrial spying is not new; in 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").
12. **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 logon IDs and passwords. The practice of "strong password" is therefore important.

13. **<u>Software piracy</u>:** 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. <u>end-user copying</u>: 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. <u>hard disk loading with illicit means</u>: hard disk vendors load pirated software;
    3. <u>counterfeiting</u>: large-scale duplication and distribution of illegally copied software;
    4. <u>Illegal downloads from the Internet</u>: by intrusion, by cracking serial numbers, etc. Beware that those who buy pirated software have a lot to lose:
        - getting untested software that may have been copied thousands of times over,
        - the software, if pirated, may potentially contain hard-drive-infecting viruses,
        - there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users,
        - there is no warranty protection,
        - there is no legal right to use the product, etc.

<u>Cybercrime against Society</u>

1. **<u>Forgery</u>:** Counterfeit currency notes, postage and revenue stamps, marksheets, etc. can be forged using sophisticated computers, printers and scanners. 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.
2. **<u>Cyberterrorism</u>:** Cyberterrorism is a controversial term. Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

3. **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.

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 topic 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.

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.
    a) One is to divide information systems into segments bordered by state boundaries (cross-border flow of information).
    b) 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 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.

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 cybercafés 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 to 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 (NCRB).

Cybercrimes: Indian Statistics:

Cybercrimes: Cases of various categories under ITA 2000: 217 cases were registered under IT Act during the year 2007 as compared to 142 cases during the previous year 2006, with an increase of 52.8%. 99 cases of the total 217 cases registered under ITA 2000 were related to obscene publication/transmission in electronic form known as cyberpornography. There were 76 cases of hacking with computer system which is related to loss/damage of computer resource/utility. India is said to be "youth country" given the population age distribution. However from cybercrime perspective, this youth aspect does not seem good as revealed by cybercrime statistics in India.

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%.Majority of the crimes out of total 339 cases registered under IPC fall under 2 categories i.e.., Forgery & Criminal breach of Trust or Fraud.

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.

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. 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.

CYBERCRIME & THE INDIAN ITA 2000

In India, the ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 in 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).

Hacking and the Indian Laws:

Section Ref. and Title	**Chapter of the Act And Title**	**Crime**	**Punishment**
Sec.43 (Penalty for damage to computer, computer system etc)	Chapter IX Penalties and Adjudication	Damage to computer system etc.	Compensation for Rs. 1 Crore
Sec.66 (Hacking with computer system)	Chapter XI Offences	Hacking (with intent or knowledge)	Fine of Rs. 2 Lakhs & Imprisonment for 3 years
Sec.67 (Publishing of information which is obscene in electronic form)	Chapter XI Offences	Publication of obscene material in electronic form	Fine of Rs. 1 Lakh & Imprisonment of 5 years and double conviction on second offence
Sec.68 (Power of controller to give directions)	Chapter XI Offences	Not complying with directions of controller	Fine upto Rs. 2 Lakhs & Imprisonment of 3 years
Sec.70 (Protected System)	Chapter XI Offences	Attempting or securing access to computer of another person without his/her knowledge	Imprisonment up to 10 Years
Sec.72 (Penalty for breach of confidentiality	Chapter XI Offences	Attempting or securing access to computer for	Fine up to Rs. 1 Lakh and Imprisonment up to

and privacy)		breaking confidentiality of the information of computer	2 Years
Sec.73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	Chapter XI Offences	Publishing false Digital Signatures, false in certain particulars	Fine of Rs.1 Lakh or imprisonment of 2 years or both
Sec.74 (Publication for fraudulent purpose)	Chapter XI Offences	Publishing of Digital Signatures for fraudulent purpose	Imprisonment for the term of 2 years and fine of Rs. 1 Lakh

Table: The key provisions under the Indian ITA 2000 (before the amendment)

A GLOBAL PERSPECTIVE ON CYBERCRIMES

In Australia, cybercrime has a narrow statutory meaning as used in the Cyber Crime 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 linkage of cybersecurity and critical infrastructure protection has become a big issue as a number of countries have began 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, 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 joint 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. More than 40 countries have ratified the Convention to date.

Cybercrime and the Extended Enterprise:

It is a continuing problem that the average user is not adequately educated to understand the threats and how to protect oneself. Actually, it is the responsibility of each user to become aware of the threats as well as the opportunities that "connectivity" and "mobility" presents them with. In this context, it is important to understand the concept of "extended enterprise." This term represents the concept that a company is made up not just of its employees, its board members and executives, but also its business partners, its suppliers and even its customers.

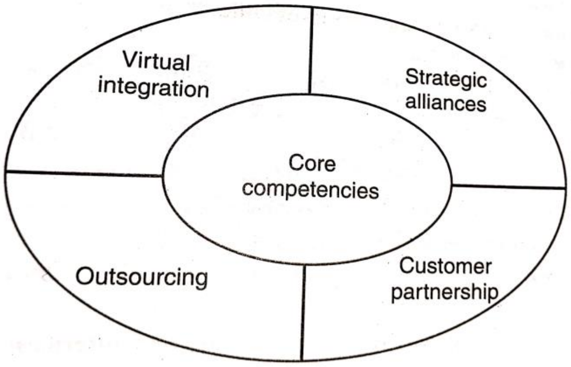


Figure: Extended Enterprise

The extended enterprise can only be successful if all of the component groups and individuals have the information they need in order to do business effectively. An extended enterprise is a **"**loosely coupled, self-organizing network**"** of firms that combine their economic output to provide **"**products and services**"** offerings to the market. Firms in the extended enterprise may operate independently. Seamless flow of "information" to support instantaneous "decision-making ability" is crucial for the "external enterprise". This becomes possible through the "interconnectedness". Due to the interconnected features of information & communication technologies, security overall can only be fully promoted when the users have full awareness of existing threats & dangers.

Given the promises and challenges in the extended enterprise scenario, organizations in the international community have a special role in sharing information on good practices and creating open and accessible enterprise information flow channels for exchanging of ideas in a collaborative manner.

CYBERCRIME ERA: SURVIVAL MANTRA FOR THE NETIZENS

The term “Netizen” was coined by Michael Hauben. Quite simply, “Netizens” are the Internet users. Therefore, by corollary, “Netizen” is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms). The 5P Netizen mantra for online security is:

a. Precaution
b. Prevention
c. Protection
d. Preservation
e. Perseverance

For ensuring cyber safety, the motto for the “Netizen” should be “Stranger is Danger!” If you protect your customer’s data, your employee’s privacy and your own company, then you are doing your job in the grander scheme of things to regulate and enforce rules on the Net through our community. NASSCOM urges that cybercrime awareness is important, and any matter should be reported at once. This is the reason they have established cyberlabs across major cities in India

More importantly, users must try and save any electronic information trail on their computers. That is all one can do until laws become more stringent or technology more advanced. Some agencies have been advocating for the need to address protection of the Rights of Netizens. There are agencies that are trying to provide guidance to innocent victims of cybercrimes. However, these NGO like efforts cannot provide complete support to the victims of cybercrimes and are unable to get the necessary support from the Police. There are also a few incidents where Police have pursued false cases on innocent IT professionals. The need for a statutorily empowered agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time.