Unit – 1

Introduction to Cybercrime

Introduction:

Definition: "Cyber security means protecting systems connected in the network, resources like hardware, software and data, from unauthorized access over the internet".

- The term "cyber" means "computer" and "security" means protection. In a wider sense one can say that cyber security is protection of computer assets or resources like data, hardware and software from unauthorized users by maintaining confidentiality, integrity and availability.
- As we know, Now-a-days everyone is aware of the internet, there is an increase in access to free websites, which gives the probability of malicious activities a higher rate through the internet known as cybercrime.
- "The malicious activities which take place with use of computers over the internet" is called cyber-crime.
- Cybercrime is a newly emerged crime to the world.
- The first cybercrime was recorded in the year 1820. It is the major attack which was recorded recently.
- Cyber criminals are technically skilled people who are about to make enormous losses to people in the society to great extent. With the increase of technology, they are able to conceal themselves from the government to a wider extent. These cyber criminals may attack in different forms in this cyber era.
- The term cybercrime is used by courts in some judgements in India. Cyber crime is an uncontrollable evil which is done by misusing growing technology on computers.
- The Internet is acting as a medium for cyber-crimes. Internet usage may increase technology and give many benefits as well as increase the rate of cyber-crimes which is a major concern now-a-days.
- Examples of cybercrimes which are in trend are cyber stalking, cyber-terrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyber defamation etc..,
- If any crime is done by use of a computer then it is also considered as a cybercrime.
- India's position is not good in cybercrimes. Government sites or corporate sites were attacked more than 780 times between February 2000 and December 2002.
- India ranks 10th in the Cybercrime Index
- If we see trends in INDIA on cyber-crimes, the rate of cyber-crime is increasing enormously.
- If we see the rate of reported cases 740,957 cases were reported in the starting four months of 2024.

The most cyber-crimes which innocent people are facing is

1. In the period 2022-2023 only financial fraud is contributing 75% of cyber-crimes.
2. In the period 2021, ransomware attack is contributing 78% of cybercrimes in Indian organizations and data encryption is contributing 80%.

Cybercrime: Definition and Origins of the word

Origin: The "Cybercrime" term was introduced by William Gibson in 1982. Even though the cyber-crime term was introduced earlier it gained popularity in 1984 by a novel called "Neuromancer".

- It takes 2 years of time for the term "Cybercrime" to get popular.
- Akash Arora (1999) was one of the earliest examples of cybercrime in India(yahoo case).
- The term **"Cybercrime"** relates to a number of other terms such as where **"Cyber"** related to **"Computer"** and **"Crime"** related to **"Bad activity** or **illegal activity".**
- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution.
- If any crime committed by use of electronic devices or in digital form (i.e., through a computer, the internet, emails, URLs, etc.), it is simply called a cybercrime.

Definition:

"Any illegal activity (or) bad activity (or) naughty activity which is committed through a computer over the internet" is called cybercrime.

Alternative definitions of Cybercrime are as follows:

1. If any financial loss is made because of computers, then it is also called cybercrime.
2. Related to any theft of hardware (or) software, encrypting the files and demanding money in the form of bitcoins called ransom is also considered cybercrime.
3. "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."

Some terms related to cybercrime are:

1.Computer-related crime

2. Computer crime

3. E-Crime

4. High-tech crime

5. Internet crime

Cybercrimes are arising faster and happening through different mediums in different forms. Some of the examples of evolving cyber-crimes are:

1. If a crime is committed by using the internet through a computer to steal someone's identity, to monitor some other person's activities through various social media platforms like Facebook, Instagram, Twitter, etc., and harass them for the sake of financial gain, to interrupt an organization's activities, or to interrupt services to the legitimate users by making the server down during peak time through malicious programs.
2. All crimes involved with computers through the internet.

As per information security, the chances for the possibility of attack because of vulnerability (weakness) with threat (a person or a competitor a tool with malicious intention to take advantage of vulnerability and to damage the computer or computer resources) in information security are increasing as growth of internet users is increasing day-by-day from the past few years, the growth of cybercrime has increased enormously to a wide range by millions of internet users.

Some people are not accepting the fact that cybercrime is a crime, as it is not a crime that is not harming any human physically.

But, legally the judiciary introduced some laws all over the world.

There is a small difference between the two terms "computer crime" and "computer fraud," which are punished.

Cybercrimes are somewhat different from traditional crimes in four ways:

a. Cybercrime is easy to commit and learn.

b. They need few resources to commit.

c. Cybercrimes are not completely illegal.

Important Definitions related to Cyber Security:

Cyberterrorism: If terrorist groups & agents use information security, then it is called Cyberterrorism.

(OR)

If any person from terrorist group or a person with terrorist intention uses the internet (or) computer (or) any electronic device to cause any interrupt to major websites (or) physical harm (or) even may cause to death of any individual (or) any group in the society is called cyberterrorism.

Case Study-1:

In the recent Ukraine-Russian war, an unknown individual launched several cyber attacks against Russian computer systems including the Russian federal executive agency which is responsible for monitoring and controlling mass media to disrupt the communication among the country.

Phishing:

Phishing is the most common type of cybercrime every individual/company is now facing. It is a cyber-crime where attacker tries to capture any individual/organizations sensitive information (or) personal confidential information by creating a fake website and sending email with the fake website link/attachment from a legitimate source by email spoofing making actual user thought like the email is from legitimate source for financial gain (or) to compromise the system.

Here, by email spoofing the attacker tries to send email from legitimate sources like bank, google accounts, organization etc.., By clicking on the fake website URL (fake website looks like legitimate website making user to believe it as legitimate website)legitimate user redirects to fake website where sensitive information of user can be captured to get financial gain.

Case study -2:

One of the Business email scam is Crelan bank in Belgium which lost more than $75 million. In this attack, the attacker got access to the accounts of senior corporate executives and instructed employees to send money to the attacker accounts. This scam was identified at the time of internal audit and unable to recover the loss.

Cyberspace:

Cyberspace is a place where two (or) more individuals from any part of the world can communicate with each other or exchange information through a computer /internet as a medium. Cyberspace uses TCP/IP to transmit data from one individual to another through a computer, which provides more reliability for effective communication (or) transmission of data.

CYBERCRIME AND INFORMATION SECURITY

When there is no security for information or data (which may include computer resources/ data), it may lead to cybercrimes. As per the amendments according to cyber laws. "Cybersecurity" means securing data, computers, computer resources, and misuse of data (like deleting, copying, or modifying) stored in computers from unauthorized access. The cybersecurity term mainly focuses on not only protecting the data from computers but also taking security measures to protect physical devices connected within the network.

Most of the financial losses are occurring because of insider threats (insider threats may be past employees/individuals within an organization like current employees/stakeholders/partners/clients who can lead to financial loss by knowingly or unknowingly). As the organizations are greatly impacted by insider threats, not only financial loss is happening but also leakage of customer data/ important data to the competitor company but companies are failing to identify the loss at that instant of time and the impact is very high. Because of this high impact for financial losses through online cybercrimes. Cybercrimes occupy a prominent role in information security as per the surveys conducted so far.

Rarely, reporting financial losses we can see from any organization. To avoid a negative image on their companies, almost every company hesitates to reveal any security incidents inside their organization.

As per the survey, it was very clear that awareness seems to be very low in terms of data privacy.

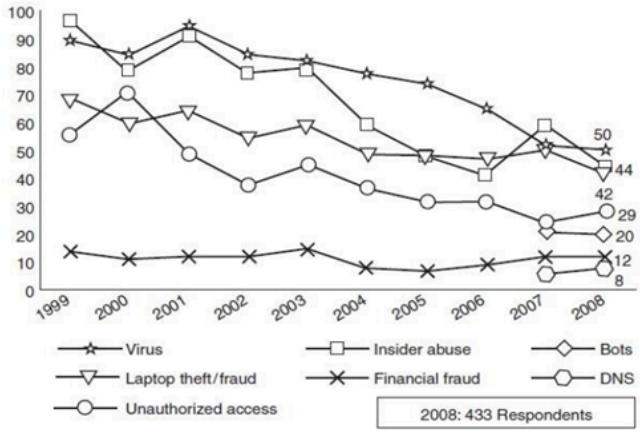

Figure: shows several categories of incidences

The Botnet Menace: Network of infected machines which are under the control of an attacker containing harmful software to create a back door or any malicious intention without actual user knowledge or consent is called a Botnet. “Network of infected machines (or) network of zombie computers is defined as “Botnet” (where zombie computer means any personal computer which is compromised and under the control of an attacker without actual user intervention).

In Botnet, all infected machines work on common command and control infrastructure where malwares run slowly to deceive an innocent individual/organization for malicious acts.

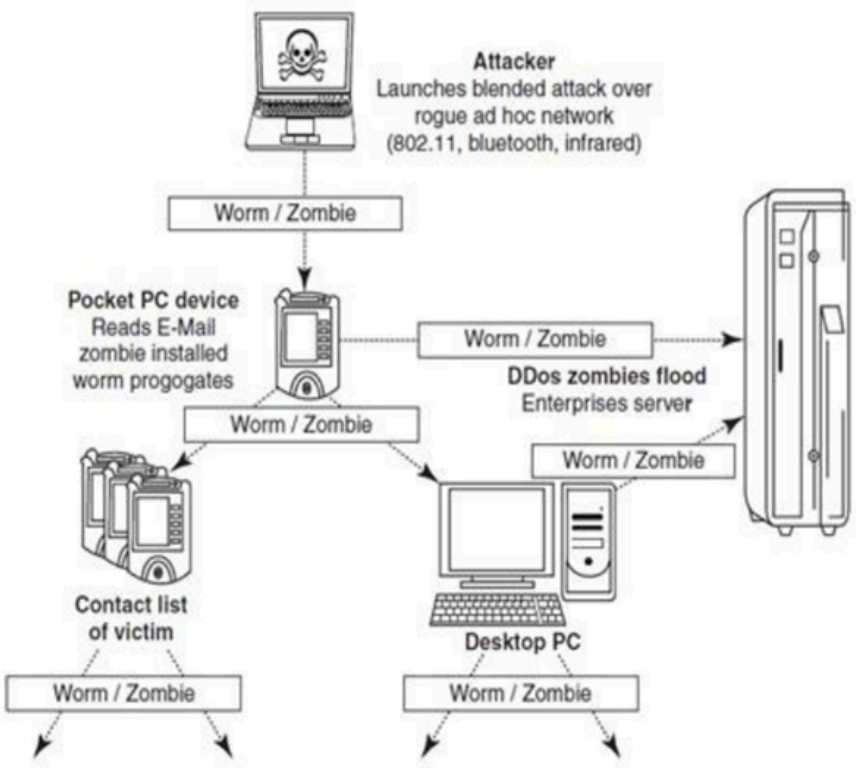

Figure: How a Zombie works

By using a botnet, an attacker can perform various malicious activities. Some of the following are:

- denial-of-service attack (DoS attack),
- Spyware,
- EMail Spam,
- Online Fraud

Initially a system gets compromised or infected by a virus or malware which contains a malicious code (short piece of code) and controlled by the attacker thereafter with commands. With a single compromised machine an attacker can infect many machines within a network (or) with the vulnerability that exists in any personal computer. Even though, after the system is infected or compromised it works as a normal computer thereafter.

By using Botnet, attackers can make the key security principles not to be achieved like confidentiality, Integrity and availability.

To overcome this one should protect their physical devices and make sure that they update patches often to close the vulnerabilities that exist in their system.

Case study – 3:

By using Botnet, 500 million Yahoo accounts were compromised in the year 2014. Passwords and basic information were stolen during the attack, but bank information was not stolen.

WHO ARE CYBERCRIMINALS?

Cybercriminals are technically skilled people who use their skill for malicious/ illegal activities are called cyber criminals.

Cybercrime involves such activities:

- Hacking;
- 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.
- Email spoofing
- Email bombing
- Spamming

Types of Cyber Criminals:

1. Type I: Cybercriminals – hungry for recognition

In Type -1, they perform cybercrimes just for the sake of recognition. IT Professionals, Hobby hackers, Political hackers, Terrorist groups fall in this category.

2. Type II: Cybercriminals – not interested in recognition

In Type – II, they perform cyber crimes or they do illegal activities but for financial gain (or) personal gain (or) for any other purpose.Psychologically unfit persons, hackers (with financial gain), state-sponsored hacking, organized criminals fall under this category.

3. Type III: Cybercriminals – the insiders

In Type – III, they perform cybercrimes to take revenge on present/former organizations for personal gain/financial gain.

CLASSIFICATIONS OF CYBER CRIMES:

Cyber-crimes are classified as follows:

- Cybercrime against individual
- Cybercrime against property
- Cybercrime against organization
- Cybercrime against society

1. Cybercrime against individual:

A. E-Mail Spoofing:

An email looks like a legitimate one from one person/organization but it came from another person. In email spoofing, the legitimate user believe that mail originated from legitimate user itself but receives from attacker making user to redirect to some other website or to download any malware, etc..,

Case study - 4:

If we consider an example, assume that Roopa and Suresh are good friends. Roopa has an E-Mail address roopa@sonixlabs.org. They came across some disputes meanwhile. Then Suresh grows furious against Roopa and spoofs her EMail and sends vulgar messages to all her friends. Since the E-Mails appear to have originated from Roopa, her friends believed that Roopa is the culprit and started hating her and kept her away by giving proper complaint on her.

In this entire scenario, Roopa is innocent and Suresh is the culprit as Suresh wants to defame Roopa; he spoofed Roopa's email and succeeded in his own way.

B. Online Frauds:

Online frauds are increasing day-by-day now-a-days. Most common forms of online frauds are through phishing and spoofing where phishing means criminal tries to capture user related sensitive information like bank account numbers, credit card numbers, usernames, passwords, etc.., by creating a fake website and sending that fake URL to targeted user/set of users either individual/organization by email by using email spoofing making user to believe that it was from genuine source and captures sensitive information. Which often results in identity theft and financial loss.

Spyware is a malicious program that is loaded onto one's computer without their knowledge. Spyware itself looks like genuine software and embeds itself into one's computer and monitors each and every activity of the user and collects sensitive information / personal confidential information.

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

Phishing is the process of capturing personal confidential information (or) sensitive information through emails/websites by looking like a genuine source. Sensitive information may include usernames, passwords, credit card numbers, etc.

Spear Phishing is sending phishing emails to specific organizations to capture sensitive information in specific to one organization specific confidential information or employee's sensitive information to do more attacks.

In spear phishing, emails has sent to all members or employees of the organization making employees believe that the mail is from a fellow employee or colleague.

Difference between Phishing and spear phishing is that in phishing, the attacker can capture sensitive information of an individual whereas in spear phishing the main goal is to access the organization's entire computer system.

Vishing (voice phishing) is a type of phishing attack which is done through voice over internet like skype. In this attack attacker calls the users and asks for confidential data from unknown numbers, fake caller id etc.., In this type of attack, attackers can get confidential data like credit card details, bank account numbers, birth dates etc..,

Smishing (SMS phishing) is a type of phishing attack where an attacker sends SMS (Shorthand message) to users with any fake website or attachment to download so that the attacker can capture sensitive information of the user , making the user believe the message is from a genuine source.

C. Spamming:

Spamming means an individual (or) attacker who sends a large or bulk number of unwanted mails (or) messages to people with unwanted information/ads etc.., randomly. Although if spam is done electronically through mails/internet forums/advertisements/facebook etc..,

Avoiding spamming is practically impossible. As the entry has no barriers. The following measures should be taken care of :

- Repeating keywords;
- use of keywords that do not relate to the content on the site;
- redirection;
- 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).

D. Cyber defamation:

Making someone or some organization defame through the computer over the internet by publishing false information or false images or false videos through any website or mails or any social media platform about an individual or organization to make bad publicity (competitors/enemies) is called cyber defamation. If someone makes someone bad by using the internet then only it is called cyber defamation.

Case study - 5:

For example, Roopa and Suresh are good friends, but as the time passes disputes arise between them and become enemies. So, Suresh wants to send a fake email to all Roopa's friend's pretending to be Roopa with email spoofing. So that all Roopa friends believe that false information as true as they got email from Roopa's personal email only.

E. **Cyberstalking and harassment:**

Cyber stalking – means following an individual/group of individuals/organization through the internet over different social media platforms secretly and harassing the individual/group of individuals/organization later for the sake of any profit like financial gain or sexual gain. Not only harassment, cyber stalking can also use some other's identity and can do any kind of activity, spreading false accusations, etc..,

Types of stalkers:

1. Online Stalkers: Interacting with the victim through the internet and getting started conversation later led to harassment.
2. Offline Stalkers: Traditional way of following an individual and monitoring all the personal activities later led to harassing manually.

F. Computer Sabotage:

Virus, Worms, Logic bombs are used to stop the normal functioning of a computer without the user's knowledge. To interrupt normal functionality, one should introduce malware containing virus, worm, logic bomb.

Virus: It is a small malicious program which infects the clean file within a computer to copy/delete/modify/damage the files/entire computer. It copies itself within a computer and is able to infect computer hardware as well.

Worm: Unlike viruses, Worm makes a copy of itself and spreads all over the computers within the network and can delete/modify/damage/copy files in those computers.

Logic bombs: Logic bomb is a piece of code with malicious intention that looks like a legitimate software but Logic bombs are active when only certain events or conditions trigger, it may take time to get logic bombs to get active. Sometimes it may take years of time also to get that logic bomb active. Some viruses are also considered as logic bombs as they lie in the system until a certain condition or event triggers.

G. Pornographic Offenses:

Child pornography means publishing any image/video of a minor and any individual if they intentionally/unintentionally force a child to do sexual activities by showcasing some interest to them under the age of 18 years is considered as an offense and crime.

H. Password Sniffing:

A special software used to capture passwords and usernames by observing the network traffic. This is most often used in public wi-fi networks where it is easy to spy and can get passwords and username as they are un-encrypted. Every time, password sniffing is not a malicious activity, sometimes it is used by IT professionals for their job purpose to ensure better security.

2. **Cybercrime against property:**

A. Credit Card Frauds:

Credit cards are the most commonly known cyber-crime to every human. As increase in technology and use of the internet for electronic transactions the rate of increase of credit card fraud increased rapidly. So collectively, in order to reduce all this kind of cyber-crimes, all banks introduced some security standards for all transactions and the user himself can send money from his account to another account only. If any individual even steals the credit card also he was unable to make the transaction because of enhanced security and necessary measures taken. But, still through phishing, vishing, smishing, credit card frauds exist. So, by proper awareness of cyber crimes among people can reduce the cyber-crimes.

B. Intellectual Property (IP) Crimes:

Now-a-days technology is growing faster, with growing technology cyber crimes are rising even faster. Among the evolving cyber crimes Intellectual property crimes is one of them. Cyber theft of Intellectual Property means stealing of copyrights, software piracy, trade secrets, patents etc., using the internet and computers.

Case study – 6: If we consider an example, we can see outside different duplicate software's available for one application or for one purpose by competing companies. Which may be a huge loss to the company who originally created it. Making piracy films which may be a huge loss to

the producer without purchasing copyrights is also an offense. As malicious activity can be performed from anywhere but impact can be more and the same. To find the culprits, it's practically very hard to find as the criminals erased the data and flew away.

C. Internet time theft:

Internet theft is also a cybercrime where any unauthorized person who uses some other individual's internet (who paid for internet hours) without their consent or knowledge. It comes like hacking because of gaining access to someone's internet by the Internet service provider's User ID and password.

3. Cybercrime against Organization:

A. Unauthorized accessing of Computer:

Unauthorized access to computers is also called Hacking. Getting unauthorized access to any individual's computer i.e., without actual user knowledge or consent with malicious intention like copying/modifying/deleting/damaging computer or computer resources or data there exists in the computer. It is definitely taking time for a person to access someone's computer but once he gets unauthorized access he will get many benefits.

B.Password Sniffing:

A special software used to capture passwords and usernames by observing the network traffic. This is most often used in public wi-fi networks where it is easy to spy and can get passwords and username as they are un-encrypted. Every time, password sniffing is not a malicious activity, sometimes it is used by IT professionals for their job purpose to ensure better security.

C. Denial-of-service Attacks (DoS Attacks):

In Dos attack Single computer system is involved in the attack. A compromised machine under the control of an attacker tries to send multiple requests to a server to flood with malicious requests making the actual or legitimate users unavailable to the service. This attack majorly focuses on making the intended service unavailable to intended users. Unauthorized access of computer resources or data will not take place in this attack.

In DDos attack two or more computer systems are involved in the attack. They send multiples and multiples of requests from compromised machines which are under the control of the attacker and make the server unavailable to legitimate users with malicious connection requests. In this attack, network traffic is flooded with malicious requests making the server down in peak times and interrupting the connection between legitimate users and a server.

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.

D. Virus attacks/dissemination of Viruses:

It is a small malicious program which infects the clean file with in a computer to copy/delete/modify/damage the files/entire computer. It copies itself within a computer and can able to infect computer hardware as well. Viruses can spread within a computer without any visible symptoms. Viruses can do some typical actions:

- Display a message to prompt an action which may set of the virus
- Misconfiguration of hardware
- Error on screen
- Shutdown system (PC)
- Just replicate themselves to propagate further harm

E. E-Mail bombing/Mail bombs:

Sending enormous (or) bombarding with multiple number of emails to an individual's account making user to overwhelm with the emails and making him to unable to access his email (or) making his email to crash so as to disrupt him from accessing his email (or) making user to do a task on repetitive basis.

F. **Salami Attack/Salami technique:**

It is a cybercrime committed for financial profit; where the loss is unpredictable by the users even if the financial loss happens at any cost.

Case study – 7:

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.

G. **Logic Bomb:**

Logic bomb is a piece of code with malicious intention that looks like legitimate software but Logic bombs are active when only certain events or conditions trigger, it may take time to get logic bombs to get active. Sometimes it may take years of time also to get that logic bomb active. Some viruses are also considered as logic bombs as they lie in the system until a certain condition or event triggers.

H. **Trojan Horse:** A Trojan Horse looks like legitimate software but facilitates unauthorized access to the user's computer system to the attacker by creating a backdoor.

I. **Software piracy:** Copying genuine software from a legitimate source without actual user's knowledge and making profit out of it simply by selling thereafter. Providing piracy software is a big offense as it can impact the legitimate user to a large extent. By using piracy software there may be chance of virus infection, no warranty, no protection, etc..,

4. Cybercrime against Society:

A.Forgery:

Forgery means duplicity of currency notes, marks sheets, revenue stamps, etc.., High Quality scanners and printers are required for forgery.

B. **Cyberterrorism:**

If terrorist groups & agents use information security then it is called Cyberterrorism. If any person from terrorist group or a person with terrorist intention uses the internet (or) computer (or) any electronic device to cause any interrupt to major websites (or) physical harm (or) even may cause to death of any individual (or) any group in the society is called cyberterrorism.

Case Study-1:

In the recent Ukraine-Russian war, an unknown individual launched several cyber-attacks against Russian computer systems including the Russian federal executive agency which is responsible for monitoring and controlling mass media to disrupt the communication among the country.

C. **Web Jacking:**

Web jacking is a cyber-crime where website control is taken by someone without user knowledge. Later the actual owner of the website does not have any more control over what appears on that website.

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.

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 of the 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 systems which are related to loss/damage of computer resources/utility. India is said to be a "youth country" given the population age distribution. However, from a 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 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).

Hacking and the Indian Laws:

Cyber-crimes are punishable under two categories:

1. The ITA 2000 and
2. The IPC

- A total of 200 cases of cybercrime were registered under the ITA act 2007 as 142 cases were registered in 2006.
- Under IPC, 339 cases were recorded in 2007 as 311 cases were recorded in 2006.

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

Sec.43 (Penalty for damage to computer, computer system etc)	Chapter IX Penalties and Adjudication	Damage to computer systems etc.	Compensation for Rs. 1 Crore
Sec.66 (Hacking with computer system)	Chapter XI Offenses	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 Offenses	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 Offenses	Not complying with directions of controller	Fine upto Rs. 2 Lakhs & Imprisonment of 3 years
Sec.70 (Protected System	Chapter XI Offenses	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 and privacy)	Chapter XI Offenses	Attempting or securing access to computer breaking confidentiality of the information of computer	Fine up to Rs. 1 Lakh and Imprisonment up to 2 Years
Sec.73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	Chapter XI Offenses	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 Offenses	Publishing of Digital Signatures for fraudulent purpose	Imprisonment for the term of 2 years and fine of Rs. 1 Lakh

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 EMail legislation in India is concerned.

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

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.

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.

CoE CyberCrime 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:

If we can see all over the world, there are less people who are aware about cybercrimes and their impact. To make people aware about cybercrimes is our primary responsibility. Make each and every human adequately knowledgeable about cyber threats and their impact. 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. It is very important to understand the term "extended enterprise". This term means a combination of employees, board members, clients, business partners and customers.

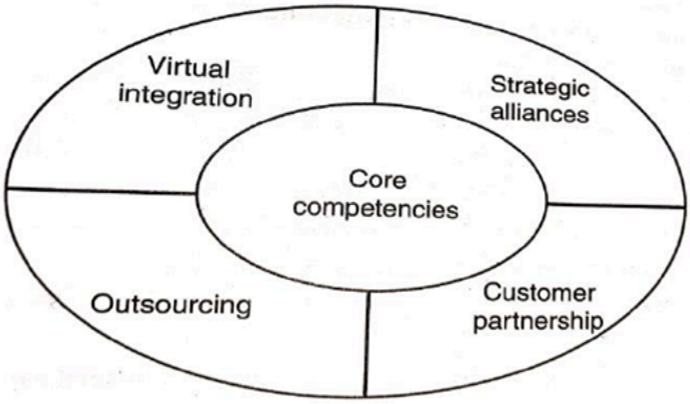

Figure: Extended Enterprise

Each and every individual within the organization or in connection with the organization has access to the information to fulfill their job role. All firms can combine their economic output to provide "products and services" offerings to the market. Firms in the extended enterprise may operate independently.

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. We can simply say, "Netizen" means 'Internet user'. Internet users are the people who spend most of their time on the internet for various activities. To protect a normal netizen from cyber threats we follow 5 P's for online security.

The 5P Netizen mantra for online security is:

1. Precaution
2. Prevention
3. Protection
4. Preservation
5. Perseverance

To ensure 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.

To ensure 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 on their computers. That is what 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.