CYBER SECURITY

INTRODUCTION TO CYBERCRIME:

- INTRODUCTION
- CYBERCRIME: DEFINITION AND ORIGIN
- CYBERCRIME AND INFORMATION SECURITY
- WHO ARE CYBERCRIMINALS?
- CLASSIFICATIONS OF CYBERCRIMES

UNIT-1

INTRODUCTION

- The phenomenal growth of Internet
- Unrestricted access to information on internet has lead to Cybercrime.
- These activities include the use of Computers, Internet, Cyberspace and the WWW.
- The Frist Recorded Cyber Crime : 1820
- Around 2328 cyber crimes are thought to occur each day. Over the last 21 years from 2001 to 2021, cyber crime has claimed at least 6.5 million victims with an estimated loss of nearly $26 billion over the same period.
- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.

INTRODUCTION (CONT..)

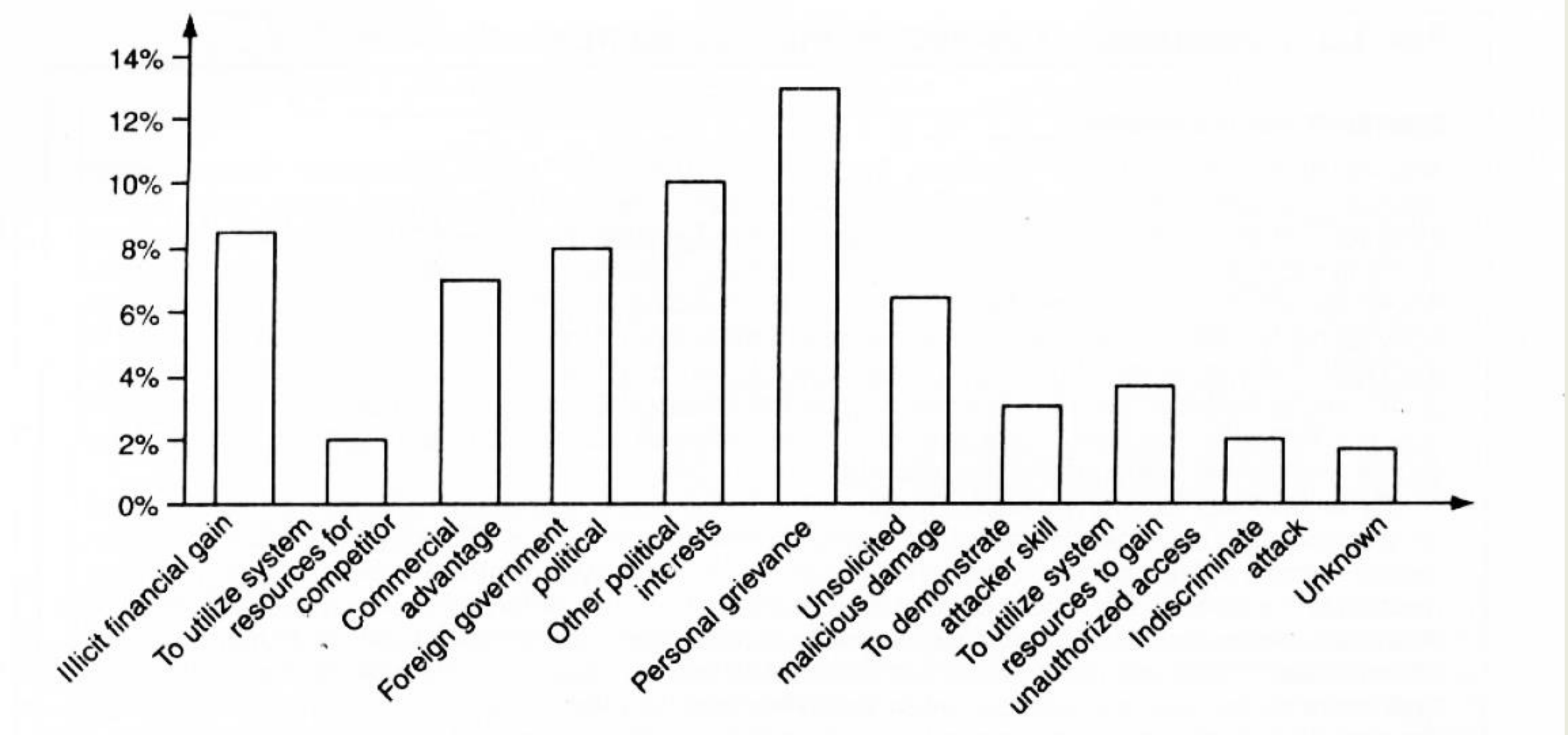


Fig: Cyber Crime Trend (2008 statistics)

CYBER CRIME: DEFINITION & ORIGINS

CYBER SECURITY

- "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.

CYBER CRIME: DEFINITION & ORIGINS (CONT..)

- "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."

- Synonyms:
  - Computer-related crime, Computer crime, Internet crime, E-crime, High-tech crime, etc.

- 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

CYBER CRIME: DEFINITION & ORIGINS (CONT..)

- Cybercrime is any criminal activity which uses network access to commit a criminal act.
- Cybercrime refers to the act of performing a criminal act using cyberspace as the communications vehicle.
- Cybercrime may be internal or external.
- Some people argue that a cybercrime is not a crime as it is a crime against software and not against a person or property.
- 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.
  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.

CYBER CRIME: DEFINITION & ORIGINS (CONT..)

- 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.
- The term ***cyber*** has some interesting synonyms: fake, replicated, pretend, imitation, virtual, computer generated. Cyber means combining forms relating to Information Technology, the Internet and Virtual Reality
- Important Definitions related to Cyber Security:

Cyber Space, Cybersquatting , Cyberpunk & Cyberwarfare, Cyberterrorism

CYBER CRIME: DEFINITION & ORIGINS (CONT..)

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.

CYBER CRIME: DEFINITION & ORIGINS (CONT..)

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 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.
- The World Intellectual Property Organization (WIPO) has also outlined anti-cybersquatting tactics. which hove been endorsed by Internet Corporation for Assigned Names and Numbers (ICANN).
- 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).

CYBER CRIME: DEFINITION & ORIGINS (CONT..)

Cyberpunk :

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

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.

CYBER CRIME: DEFINITION & ORIGINS (CONT..)

Cyberterrorism :

- 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."**

CYBERCRIME AND INFORMATION SECURITY

- Lack of information security gives rise to cybercrimes.
- 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.

CYBERCRIME AND INFORMATION SECURITY (CONT..)

- 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.

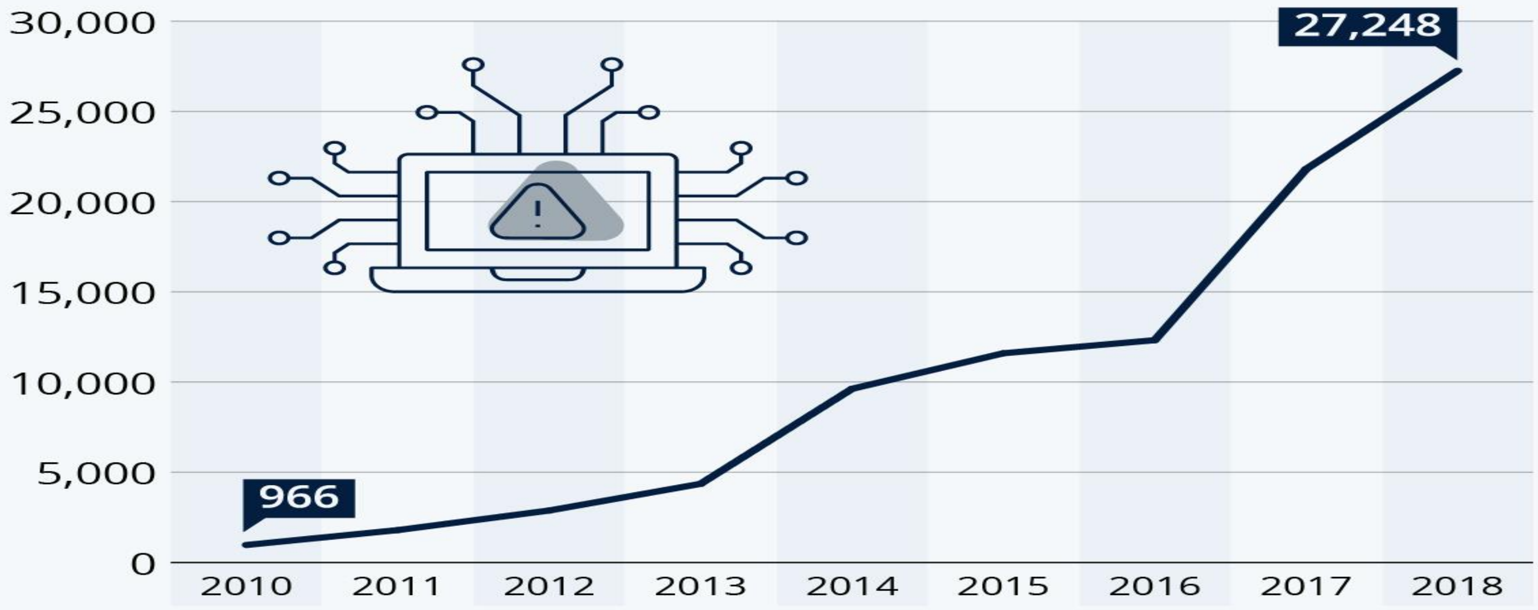
CYBERCRIME AND INFORMATION SECURITY (CONT..)

- 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.
- 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.
- Several categories of incidences include - *viruses, insider abuse, laptop theft* and *unauthorized access* to systems, implications in mobile computing paradigm, Typical network misuses are for Internet radio/screaming audio, screaming video, file sharing, instant messaging and online gaming

CYBERCRIME STATISTICS

Sharp Increase of Cyber Crime in India During Last Decade

Recorded cyber crime cases in India (2010-2018)

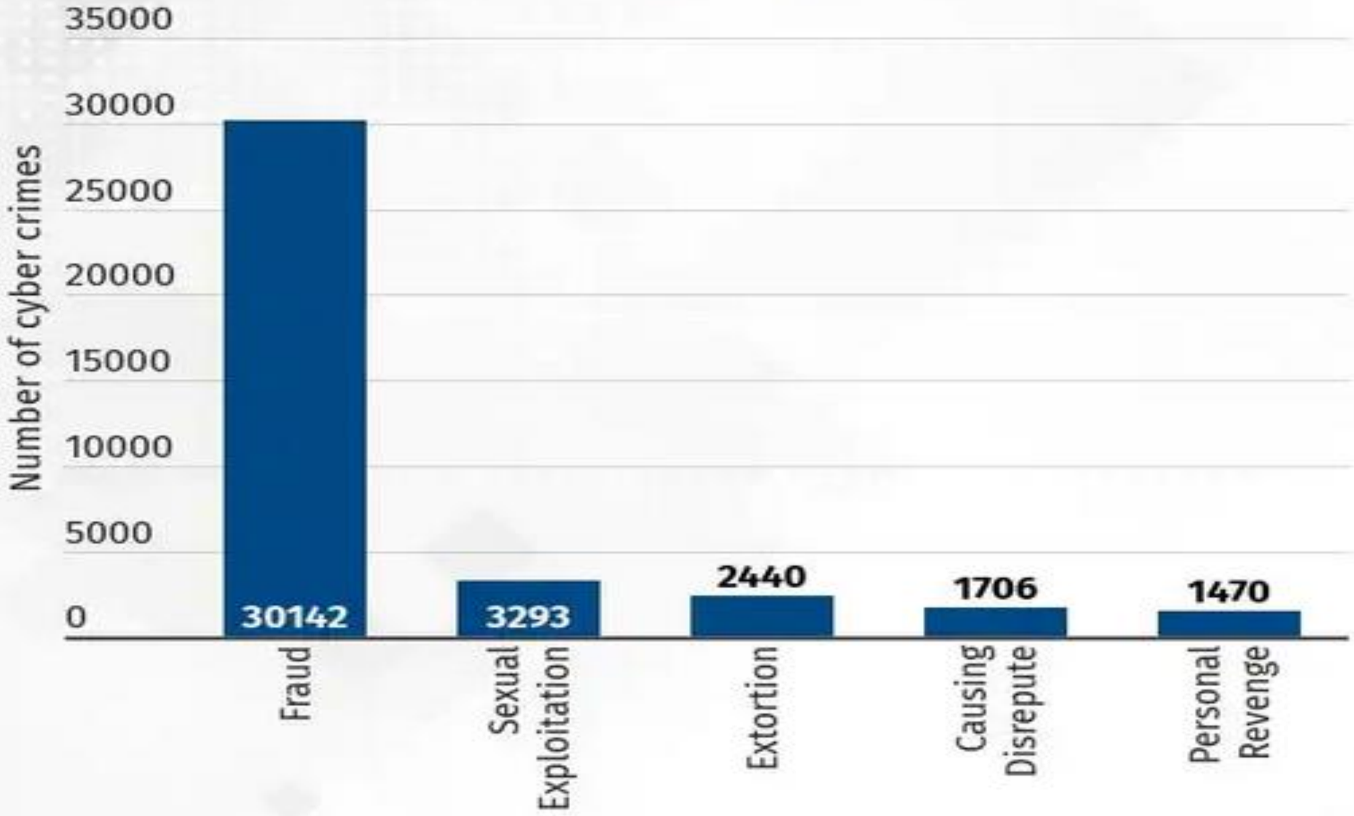


Source: National Crime Records Bureau of India

statista

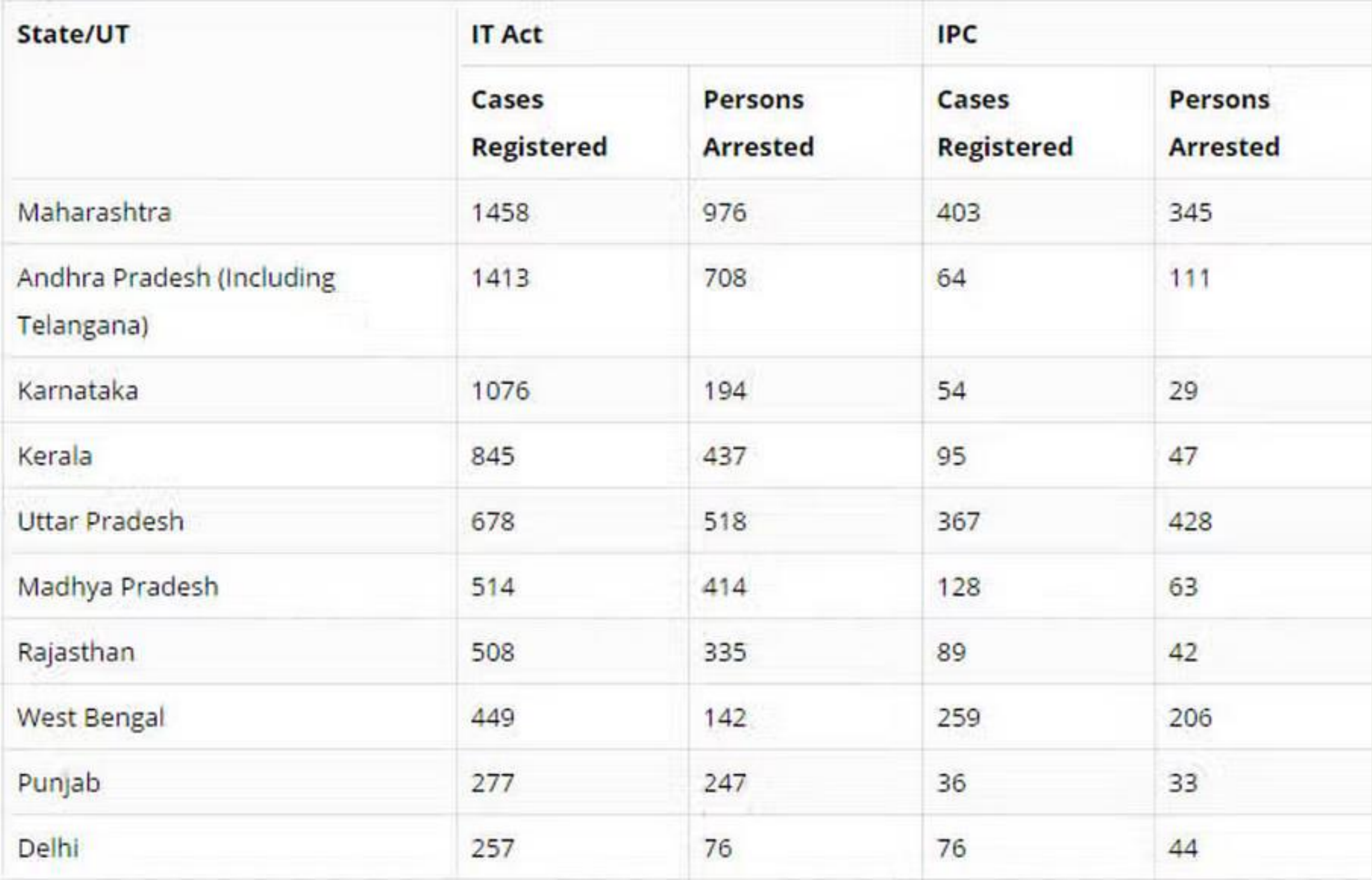
CYBERCRIME STATISTICS

TOP 5 MOTIVES FOR COMMITTING CYBER CRIMES IN 2021



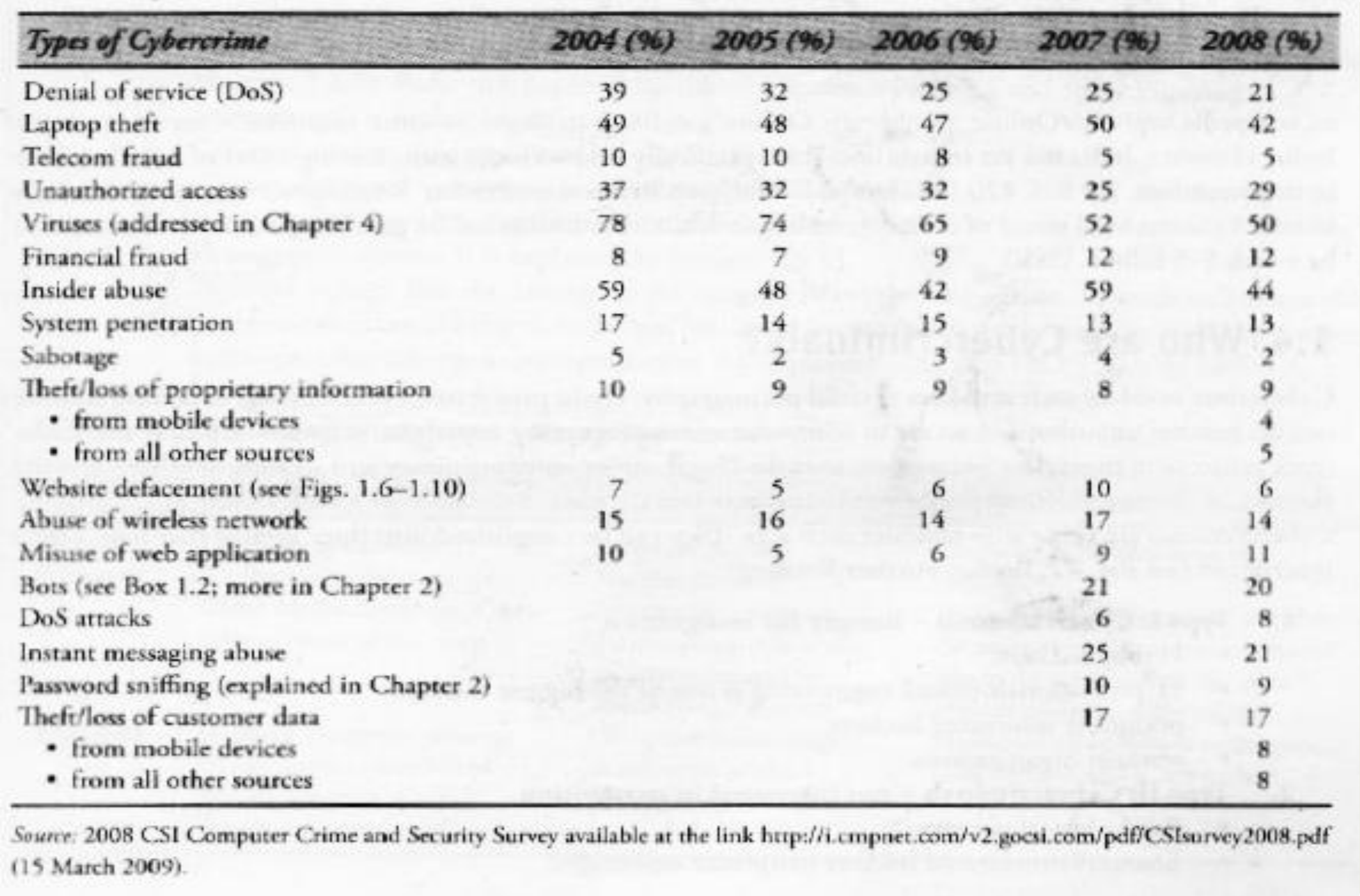
Source: National Crime Records Bureau

CYBERCRIME STATISTICS



State/UT	IT Act		IPC	
	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
Maharashtra	1458	976	403	345
Andhra Pradesh (Including Telangana)	1413	708	64	111
Karnataka	1076	194	54	29
Kerala	845	437	95	47
Uttar Pradesh	678	518	367	428
Madhya Pradesh	514	414	128	63
Rajasthan	508	335	89	42
West Bengal	449	142	259	206
Punjab	277	247	36	33
Delhi	257	76	76	44

CYBERCRIME STATISTICS

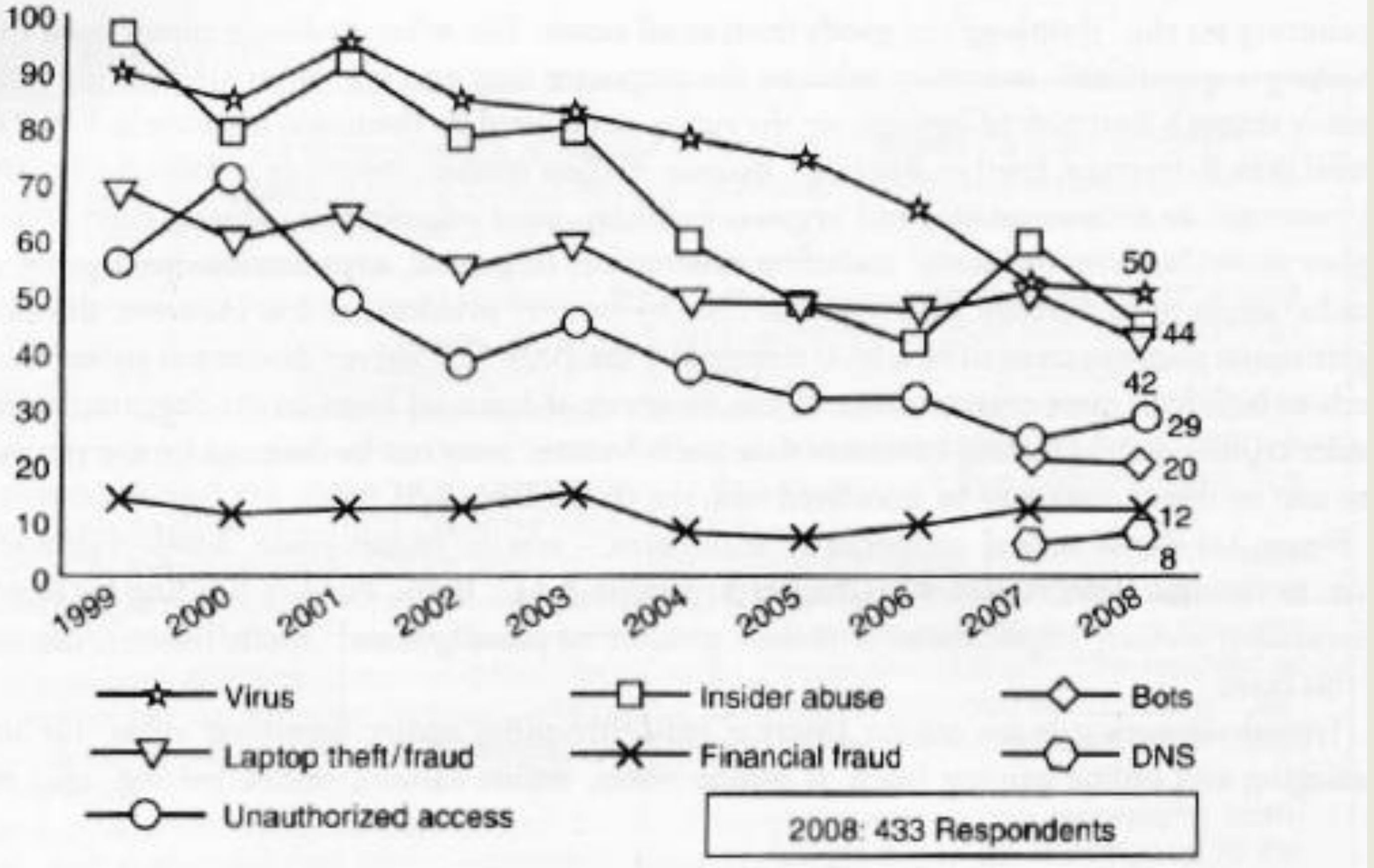


Types of Cybercrime	*2004 (%)*	*2005 (%)*	*2006 (%)*	*2007 (%)*	*2008 (%)*
Denial of service (DoS)	39	32	25	25	21
Laptop theft	49	48	47	50	42
Telecom fraud	10	10	8	5	5
Unauthorized access	37	32	32	25	29
Viruses (addressed in Chapter 4)	78	74	65	52	50
Financial fraud	8	7	9	12	12
Insider abuse	59	48	42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

Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

CYBERCRIME STATISTICS

CYBER SECURITY



Major types of incidents by percentage.

Source: 2008 CSI Computer Crime and Security Survey available at the link http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf (15 March 2009).

WHO ARE CYBER CRIMINALS?

- Cybercrime involves such activities as child pornography; 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) co perform criminal acts.
- Cybercriminals are those who conduce such acts.
- They can be categorized into three groups that reflect their motivation:
  - **Type I: Cybercriminals- hungry for recognition**
  - **Type II: Cybercriminals - not interested in recognition**
  - **Type III: Cybercriminals - the insiders**

WHO ARE CYBER CRIMINALS? (CONT..)

Type I: Cybercriminals- hungry for recognition

- Hobby hackers;
- IT professionals (social engineering is one of the biggest threat);
- politically motivated hackers;
- terrorist organizations.

Type II: Cybercriminals - not interested in recognition

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

Type III: Cybercriminals - the insiders

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

WHO ARE CYBER CRIMINALS? (CONT..)

- Thus, the typical "motives" behind cybercrime seem to be greed, desire to gain power and/or publicity, desire for revenge, a sense of adventure, looking for thrill to access forbidden information, destructive mindset and *desire* to sell network security services.

- Cybercafes are known to play role in committing cybercrimes.

CLASSIFICATIONS OF 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 offender 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

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Cybercrime against individual :

- Electronic mail (E-Mail) Spoofing and other online frauds
- Phishing, Spear Phishing and various forms
- Spamming
- Cyberdefamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offenses
- Password sniffing

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

CYBER SECURITY

Cybercrime against individual :

Electronic mail (E-Mail) Spoofing:

- A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source.

Phishing, Spear Phishing and various forms:

- **Phishing** is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate.
- **Spear Phishing** is a method of sending a Phishing message to a particular organization to gain organizational information for more targeted social engineering.
- **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.
- **Smishing** (SMS phishing) is a type of phishing attack conducted using SMS (Short Message Services) on cell phones.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Spamming:

- Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unrequested bulk messages indiscriminately.
- Examples: email spam, 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. Spammers are numerous; the volume of unrequested mail has become very high because the barrier to entry is low.
- Search Engine Spamming: Use of Subversive techniques to ensure that their site is more frequent – penalties are imposed on such activities

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Cyber defamation :

- It is a cognizable (Software) offense. “Whoever, by words either spoken(libel) or intended to be read(slander), 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.
- Punishable under IPC Section 499.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Cyber stalking and harassment :

- Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.
- Cyberstalking may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Computer sabotage:

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

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Pornographic offenses:

- Child pornography means any visual depiction, including but not limited to the following:

  1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
  2. film, video, picture;
  3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

- 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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Password sniffing:

- It 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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Cybercrime against Property:

- Credit Card Frauds
- Intellectual Property (IP) Crimes
- Internet time theft

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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 authorized, where the genuine customer themselves processes a payment to another account which is controlled by a criminal, or unauthorized, where the account holder does not provide authorization for the payment to proceed and the transaction is carried out by a third party.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Cybercrime against Organization:

- Unauthorized accessing of Computer
- Password Sniffing
- Denial-of-service Attacks (DoS Attacks)
- Virus attacks/dissemination of Viruses
- E-Mail bombing/Mail bombs
- Salami Attack/Salami technique
- Logic Bomb
- Trojan Horse
- Data Diddling
- Newsgroup Spam/Crimes emanating from Usenet newsgroup
- Industrial spying/Industrial espionage
- Computer network intrusions
- Software piracy

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Industrial spying/Industrial espionage

- 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”).

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Software piracy

- This is a big challenge area indeed. Cybercrime investigation cell of India defines “software piracy” as theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. There are many examples of software piracy:
  - end-user copying: friends loaning disks to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses;
  - hard disk loading with illicit means: hard disk vendors load pirated software;
  - counterfeiting: large-scale duplication and distribution of illegally copied software;
  - Illegal downloads from the Internet: by intrusion, by cracking serial numbers, etc.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Cybercrime against Society:

- Forgery
- Cyberterrorism
- Web Jacking

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Forgery

- 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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

Cyberterrorism

- 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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.

CLASSIFICATIONS OF CYBERCRIMES (CONT..)

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.