Module 4

Introduction to Cybercrime

- 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
- Cyber offenses: How Criminals Plan Them: How Criminals Plan the Attacks
- Social Engineering
- Cyber stalking, Cybercafe and Cybercrimes.

Introduction to Cybercrime

- Phenomenal growth of internet – unrestricted number of free websites – leading to exploitation of resources – cybercrime
- activities involve the use of computers, the Internet, cyberspace and world wide web
- 1820
- Cyber refers to fake, replicated, pretend, imitation, virtual, computer generated.

Cybercrime: Definition and Origins of the Word

- *“a crime conducted in which a computer was directly and significantly instrumental”*
- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution.
- 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.
- Any financial dishonesty that takes place in a computer environment.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.
- 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.

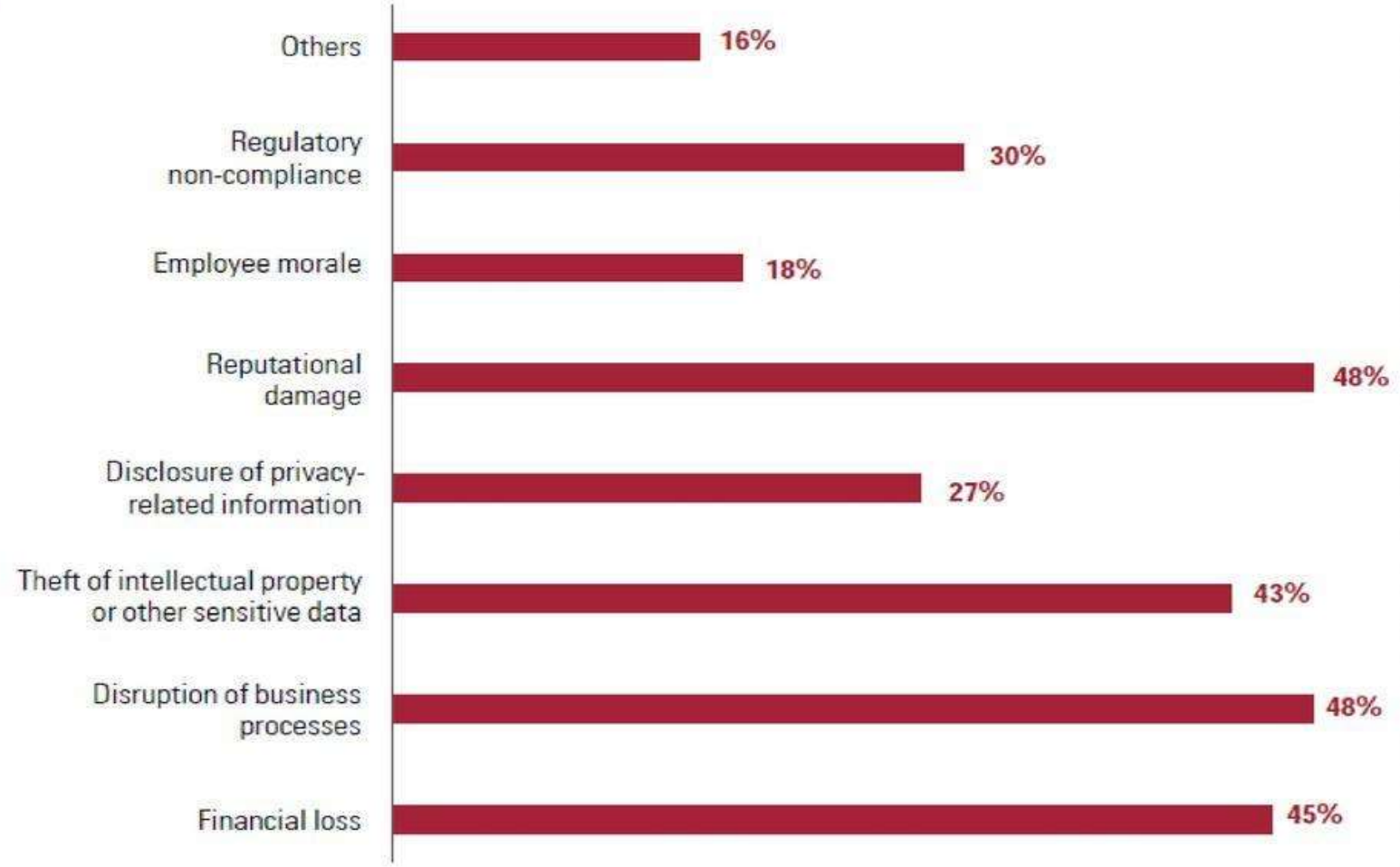
- Computer-related crime, Computer crime, Internet crime, E-crime, High-tech crime, etc. are the other synonymous terms
- A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs.
- Crimes completed either on or with a computer.
- Any illegal activity done through the Internet or on the computer.
- All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

- *Cybercrime refers to the act of performing a* criminal act using cyberspace as the communications vehicle
- "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.
- Types of attack:
  - Techno crime
  - Techno vandalism

- Techno – crime:
  - 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 24 × 7 connection to the Internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, “finger prints.”
- 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.

- Cyber terrorism 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 cyber terrorism.*"
- Difference between cybercrime and terrestrial crime:
  - how to commit them is easier to learn,
  - they require few resources relative to the potential damage caused
  - they can be committed in a jurisdiction without being physically present in it
  - they are often not clearly illegal.

Survey result - Impact of cybercrime in India



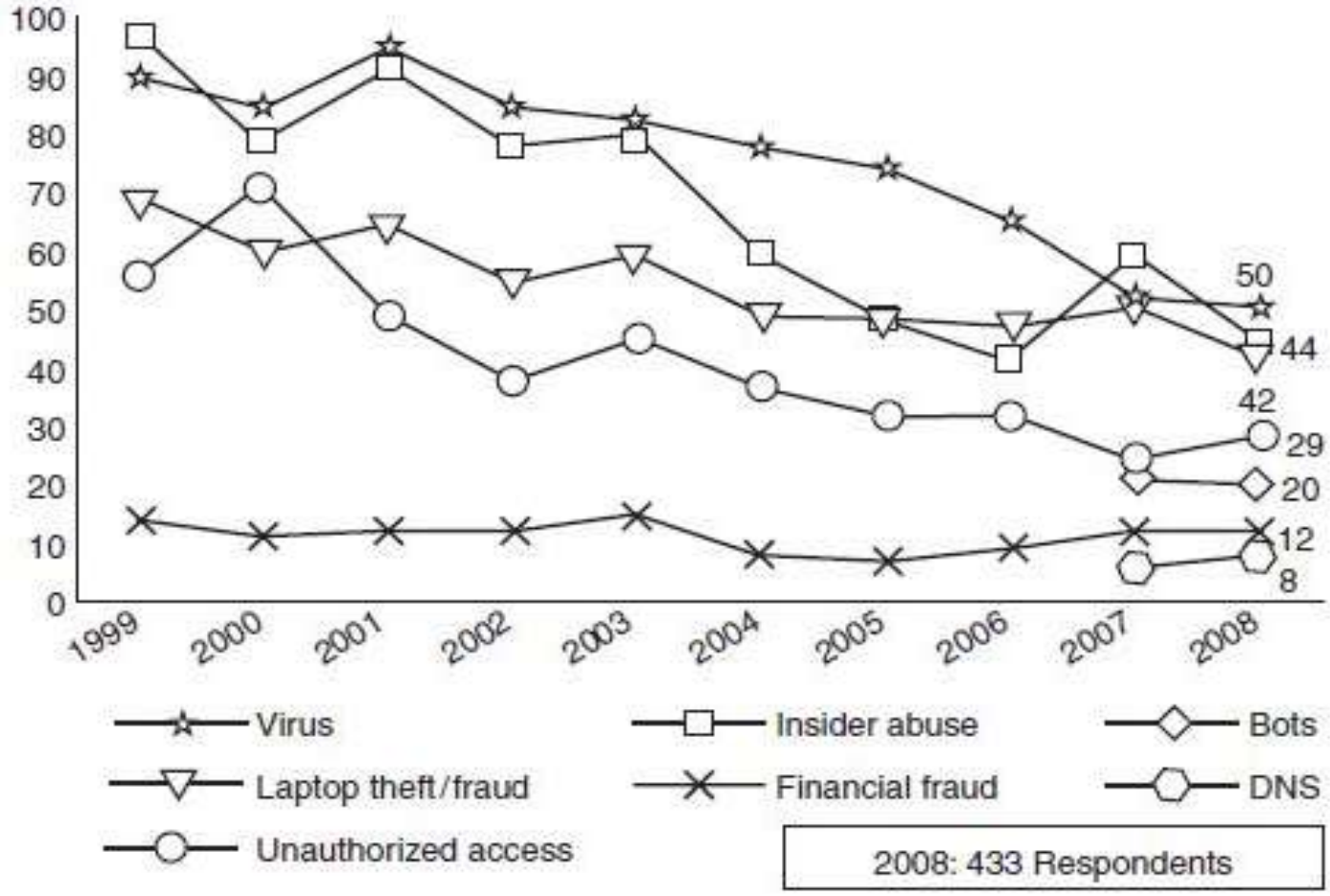
Source: Cybercrime survey report 2014, KPMG in India

Cyber crime and Information security

- Lack of information security gives rise to cybercrime
- “Cybersecurity” means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction
- Concerned with the physical security of devices along with data stored within

Challenges for securing data

- Cybercrimes occupy an important space in information security domain because of their impact – leaking customer data
- Most organizations do not explicitly incorporate the cost of the vast majority of computer security incidents into their accounting
- attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost
- Awareness about “data privacy” too tends to be low in most organizations.



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).

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

- network misuses can be found in Internet radio/streaming audio, streaming video, fi le sharing, instant messaging and online gaming (such as online poker, online casinos, online betting)

Who are Cybercriminals

- Cybercriminals are those who conduct:
  - 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

Categorization of Cybercriminals

- **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.

- Motives for cybercrime:
  - Greed
  - desire to gain power and/or publicity
  - Desire for revenge
  - a sense of adventure
  - looking for thrill to access forbidden information
  - destructive mindset
  - desire to sell network security services.

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 off ender liable to punishment by that law”
- Classified as:
  - Cybercrime against individual
  - Cybercrime against property
  - Cybercrime against organization
  - Cybercrime against Society
  - Crimes emanating from Usenet newsgroup

Cybercrime against individual

- *Electronic mail (E-Mail) Spoofing and other online frauds*.
- *Phishing, Spear Phishing and its various other forms such as Vishing and Smishing*
- *Spamming*
- *Cyberdefamation*
- *Cyberstalking and harassment*
- *Computer sabotage*
- *Pornographic offenses*
- *Password sniffing*
- use of password could be by an individual for his/her personal work or the work he/she is doing using a computer that belongs to an organization

Cybercrime against property

- Credit card frauds
- Intellectual property (IP) crimes
- Internet time theft

Cybercrime against organization

- Unauthorized accessing of computer
- Password sniffing
- Denial-of-service attacks
- Virus attack/dissemination of viruses
- E-Mail bombing/mail bombs
- Salami attack/Salami technique
- Logic bomb
- Trojan Horse
- Data diddling
- Crimes emanating from Usenet newsgroup
- Industrial spying/industrial espionage
- Software piracy
- Computer network intrusions

Cybercrime against Society

- Forgery
- Cyberterrorism
- Web jacking

Crimes emanating from Usenet newsgroup

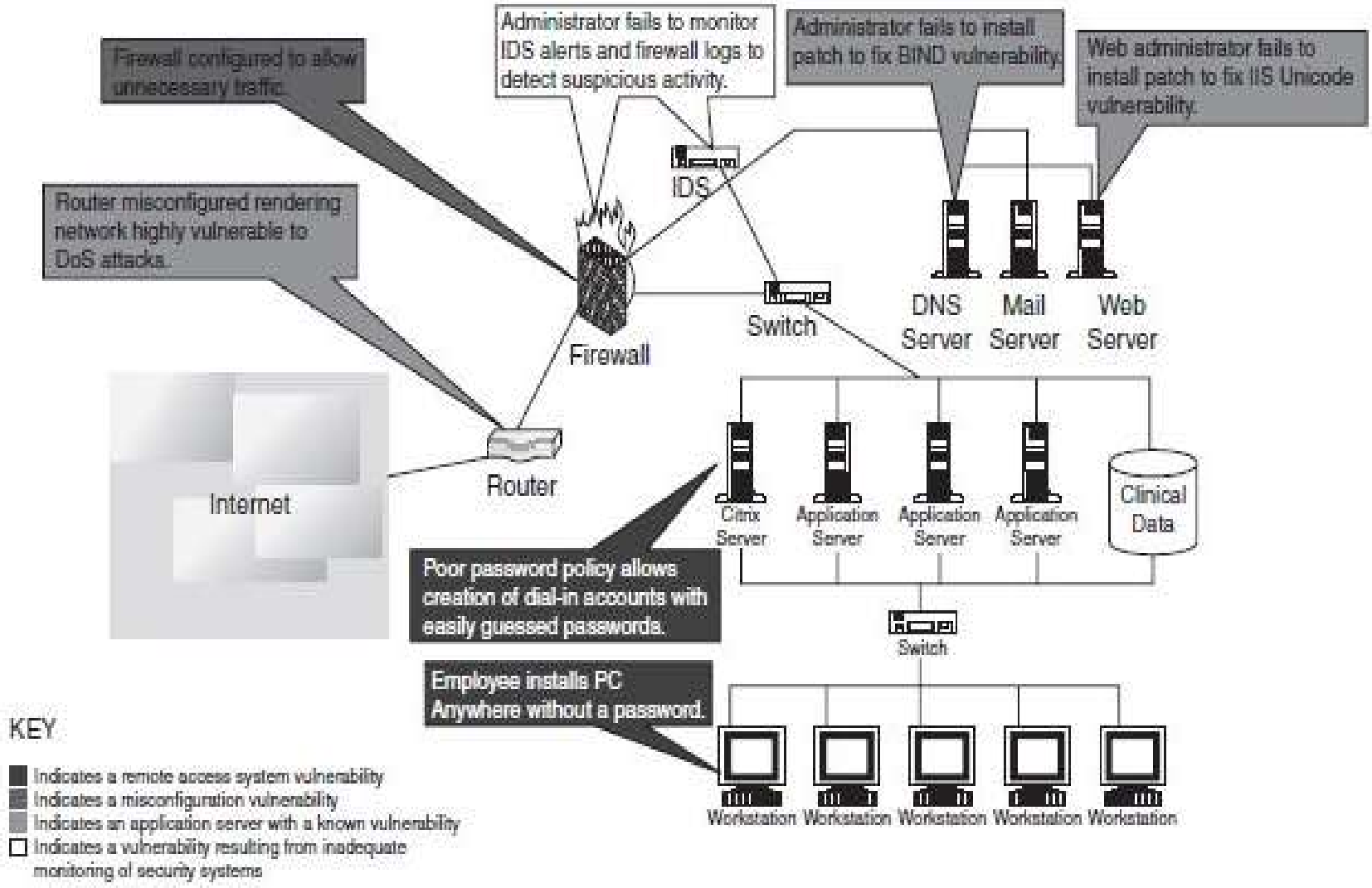
- Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way.

Module 4

Cyber offenses: How Criminals Plan Them

Introduction

- Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information.
- This is because criminals take advantage of the widespread lack of awareness about cybercrimes and cyberlaws
- An attacker would look to exploit the vulnerabilities in the networks – adequately protected


Firewall configured to allow unnecessary traffic.
Administrator fails to monitor IDS alerts and firewall logs to detect suspicious activity.
Administrator fails to install patch to fix BIND vulnerability.
Web administrator fails to install patch to fix IIS Unicode vulnerability.
Router misconfigured rendering network highly vulnerable to DoS attacks.
IDS
Firewall
Switch
DNS Server
Mail Server
Web Server
Internet
Router
Citrix Server
Application Server
Application Server
Application Server
Clinical Data
Poor password policy allows creation of dial-in accounts with easily guessed passwords.
Switch
Employee installs PC Anywhere without a password.
Workstation
Workstation
Workstation
Workstation
Workstation
KEY
Indicates a remote access system vulnerability
Indicates a misconfiguration vulnerability
Indicates an application server with a known vulnerability
Indicates a vulnerability resulting from inadequate monitoring of security systems

- The categories of vulnerabilities that hackers search for are:
  - Inadequate border protection
  - remote access servers (RASs) with weak access controls
  - application servers with well-known exploits
  - misconfigured systems and systems with default configurations

- Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them.
- Brute force hacking: It is a technique used to find passwords or encryption keys. Brute force hacking involves trying every possible combination of letters, numbers, etc., until the code is broken
- Cracker: A cracker is a person who breaks into computers - crimes include vandalism, theft and snooping in unauthorized areas.
- Cracking: It is the act of breaking into computers
- Cracker tools: These are programs used to break into computers
- Phreaking: This is the notorious art of breaking into phone or other communication systems
- War dialer: It is program that automatically dials phone numbers looking for computers on the other end

Categories of Cybercrime

- Broad categorization:
  - target of the crime
  - whether the crime occurs as a single event or as a series of events.
- Cybercrime can be categorized based on:
  - Crimes targeted at individuals
  - Crimes targeted at property
  - Crimes targeted at organizations
  - Single event of cybercrime
  - Series of events

Crimes targeted at individuals

- Exploit human weakness such as greed and naivety
- Ex: financial frauds, sale of non-existent or stolen items, child pornography, copyright violation, harassment
- With the development in the IT and the Internet; thus, criminals have a new tool that allows them to expand the pool of potential victims

Crimes targeted at property

- includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable medias like CDs and pen drives
- transmitting harmful programs that can disrupt functions of the systems and/or can wipe out data from hard disk, and can create the malfunctioning of the attached devices in the system such as modem, CD drive

Crimes targeted at organizations

- Cyberterrorism
- Attackers use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information
- damage the programs and files or plant programs to get control of the network and/or system

- **Single event of cybercrime:**
  - single event from the perspective of the victim
  - Ex: unknowingly open an attachment that may contain virus that will infect the system
- **Series of events**
  - attacker interacting with the victims repetitively
  - Ex: attacker interacts with the victim on the phone and/or via chat rooms to establish relationship first and then they exploit that relationship to commit the sexual assault

How Criminals Plan the Attacks

- Criminals plan passive and active attacks
  - Active attacks are usually used to alter the system while passive attacks attempt to gain information about the target
  - Active attacks may affect the availability, integrity and authenticity of data
  - Passive attacks lead to breaches of confidentiality
- Attacks can be categorized as either inside or outside.
  - An attack originating and/or attempted within the security perimeter of an organization is an inside attack
  - outside attack is attempted by a source outside the security perimeter
  - maybe attempted by an insider and/or an outsider, who is indirectly associated with the organization - attempted through the Internet or a remote access connection.

- Phases involved in planning cybercrime are:
  - Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
  - Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
  - Launching an attack (gaining and maintaining the system access)

Reconnaissance

- an act of reconnoitering – explore, often with the goal of finding something or somebody
- Begins with foot printing –
  - is the preparation toward pre attack phase,
  - involves accumulating data about the target's environment
  - find ways to intrude into that environment
  - Foot printing gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities
- The objective of this phase is to understand the system, its networking ports and services, and other aspects related to security that are needful for launching the attack.
- Information gathering can be done in two phases: passive and active attacks

Passive Attacks

- gathering information about a target without his/her knowledge
- usually done using Internet searches or by Googling an individual or company to gain information
  - Google or Yahoo search
  - Surfing online community groups
  - Organization's website
  - Blogs, newsgroups, press releases
  - Going through the job postings in particular job profiles for technical persons
  - Network sniffing

Active Attacks

- An active attack involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.
- It involves the risk of detection
- Active reconnaissance can provide confirmation to an attacker about security measures in place
- Tools used during active attacks: DNStracer, Hackbot, Hunt, SMBclient, TCPdump, TCPreplay

Scanning and Scrutinizing Gathered Information

- Scanning - examine intelligently while gathering information about the target
- The objectives of scanning are as follows:
  - **Port scanning: Identify open/close ports and services.**
  - **Network scanning: Understand IP Addresses and related information about the computer network** systems.
  - **Vulnerability scanning: Understand the existing weaknesses in the system.**

- The scrutinizing phase is always called “enumeration” in the hacking world.
- Objective is to identify:
  - The valid user accounts or groups
  - network resources and/or shared resources
  - OS and different applications that are running on the OS

- **Attack -** After the scanning and enumeration, the attack is launched using the following steps
  - Crack the password
  - exploit the privileges
  - execute the malicious commands/applications
  - hide the files
  - cover the tracks – delete the access logs, so that there is no trail illicit activity.

Social Engineering

- Social engineering is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders
- The goal of a social engineer is to fool someone into providing valuable information or access to that information

Classification of Social Engineering

- Human-Based Social Engineering
  - Impersonating an employee or valid user
  - Posing as an important user
  - Using a third person
  - Calling technical support
  - Shoulder surfing
  - Dumpster diving
- Computer-Based Social Engineering
  - Fake E-Mails
  - E-Mail attachments
  - Pop-up windows

Cyberstalking

- Stalking is act or process of following prey stealthily – trying to approach somebody or something
- 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
- Refers to use of Internet and/or other electronic communications devices to stalk another person

- Includes:
  - false accusations,
  - monitoring,
  - transmission of threats,
  - ID theft,
  - damage to data or equipment,
  - solicitation of minors for sexual purposes,
  - gathering information for harassment purposes
- involves harassing or threatening behavior that an individual will conduct repeatedly, for example,
  - following a person,
  - visiting a person's home and/or at business place,
  - making phone calls,
  - leaving written messages,
  - vandalizing against the person's property.

Types of Stalkers

- **Online stalkers**
  - The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.
- **Offline stalkers**
  - The victim is not aware that the Internet has been used to perpetuate an attack against them

How Stalking Works?

- Personal information gathering about the victim
- Establish a contact with victim through telephone/cell phone.
- Stalkers will almost always establish a contact with the victims through E-Mail
- Some stalkers keep on sending repeated E-Mails asking for various kinds of favors
- The stalker may post the victim's personal information on any website related to illicit services
- Whosoever comes across the information, start calling the victim on the given contact details
- Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic sites

Cybercafe and Cybercrimes

- Cybercriminals prefer cybercafes to carry out their activities
- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through
- Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week

- Pirated software(s)
- Antivirus software is found to be not updated
- Several cybercafes had installed the software called “Deep Freeze” for protecting the computers from prospective malware attacks
- Annual maintenance contract (AMC) found to be not in a place for servicing the computers
- Pornographic websites
- Cybercafe owners have very less awareness about IT Security and IT Governance

- Tips for safety and security while using the computer in a cybercafe:
  - Always logout
  - Stay with the computer
  - Be alert
  - Avoid online financial transactions
  - Change passwords
  - Virtual keyboard
  - Security warnings