CS Module 1 QB Solutions

1. Define Cyber Security and Cyber Crime.
   Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
   Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them.

2. List out the other terms of cyber crime.
   Cybercrime can sometimes be called as computer-related crime, computer crime, E-crime, Internet crime, High-tech crime, etc.

3. Define Cyber terrorism, Cybernetics, Phishing, Cyberspace, Cyber squatting, Cyber punk, Cyber warfare.

Important Definitions related to Cyber Security

a. Cyber terrorism

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."

b. Cybernetics

This term owes its origin to the word "cybernetics" which deals with information and its use; cybernetics is the science that overlaps the fields of neurophysiology, information theory, computing machinery and automation. Cyber terrorists usually use computer as a tool, target for their unlawful act to gain information

c. "Phishing"

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

d. Cyberspace

"Cyberspace" is where users mentally travel through matrices of data. Conceptually "cyberspace" is the "nebulous place" where humans interact over computer networks. Cyberspace is most definitely a place where you chat, explore, research and play.

e. Cyber squatting

The term is derived from "squatting" which is the act of occupying an abandoned space/ Building that the user does not own, rent or otherwise have permission to use.
Cyber squatting 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.

f. Cyber punk

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

g. Cyber warfare

Cyber warfare means information attacks against an unsuspecting opponent's computer Networks, destroying and paralyzing nations.
This perception seems to be correct as the terms cyber warfare and cyber terrorism have got historical connection in the context of attacks against infrastructure.

4. Explain the relationship between Cybercrime and Information Security.

Cybercrime and Information Security

The two terms are not the same

1.Lack of information security gives rise to cybercrimes.

2.From an Indian perspective, the new version of the Act (referred to as ITA 2008) provides anew focus on "Information Security in India."

3.The term incorporates both the physical security of devices as well as the information stored therein.

4. Information security primarily refers to protecting the confidentiality, integrity, and availability of data, no matter its form

CIA

Integrity - guarding against improper information modification or destruction,

Confidentiality - preserving authorized restrictions on access and disclosure,

Availability - timely and reliable access to and use of information.

5. **Cybercrime** is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, **cybercrime** is committed by **cybercriminals** or hackers who want to make money. **Cybercrime** is carried out by individuals or organizations.

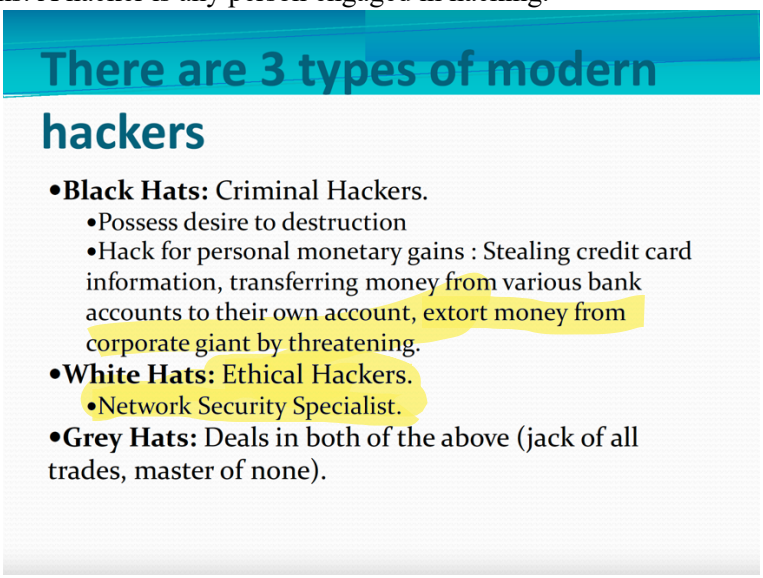
6. financial losses to the organization- data theft.

5. Who are called Cybercriminals?

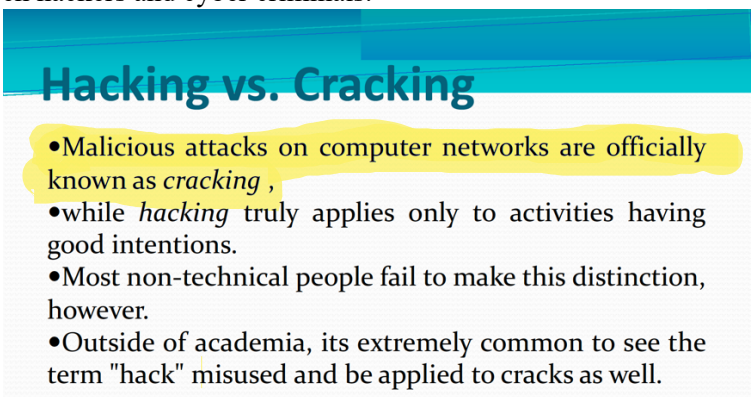
1.4 Who are Cybercriminals?

- Are those who conduct acts such as:
  - Child pornography
  - Credit card fraud
  - Cyberstalking
  - Defaming another online
  - Gaining unauthorized access to computer systems
  - Ignoring copyrights
  - Software licensing and trademark protection
  - Overriding encryption to make illegal copies
  - Software piracy
  - Stealing another's identity to perform criminal acts

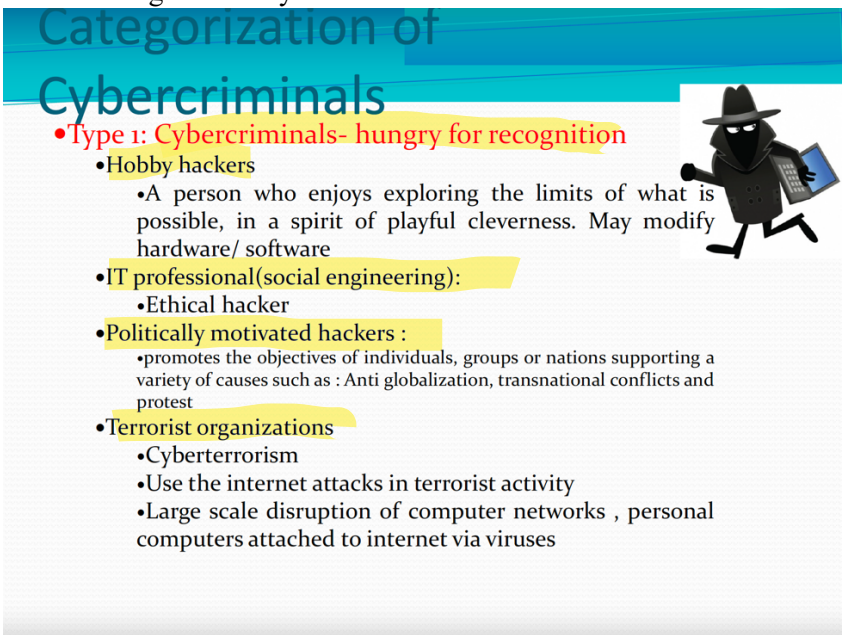
6. Define hackers and its type.
Hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking.

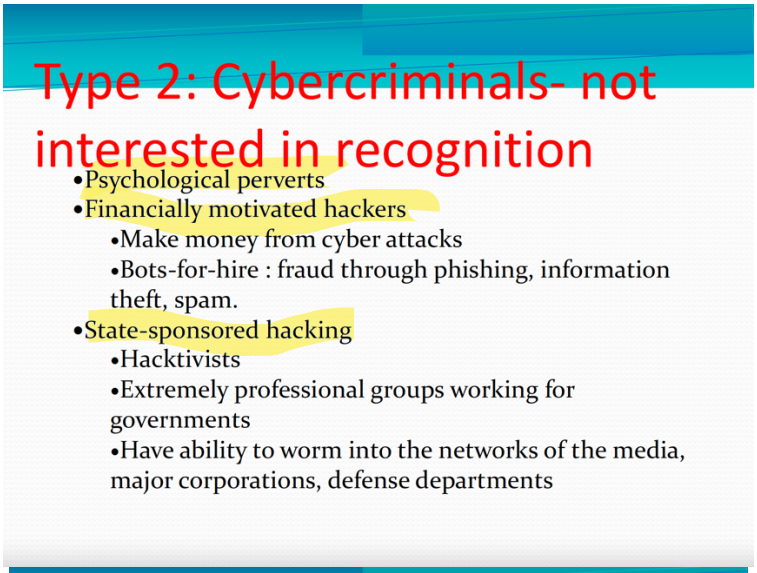


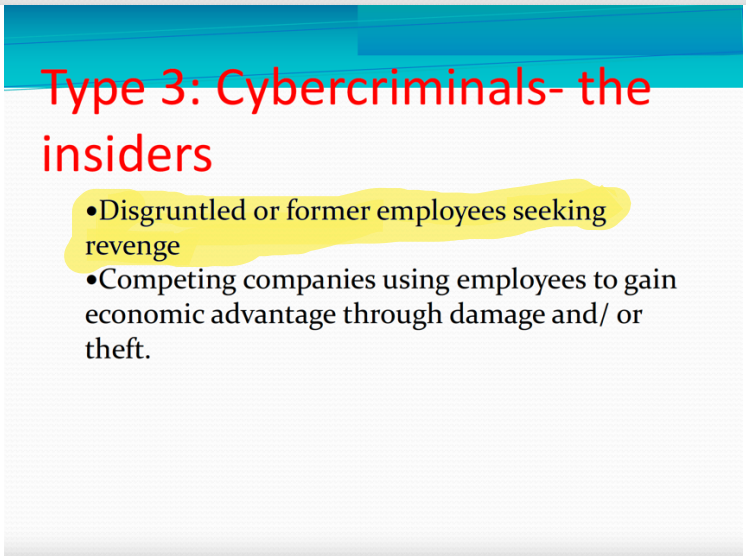
7. Difference between hackers and cyber criminals.



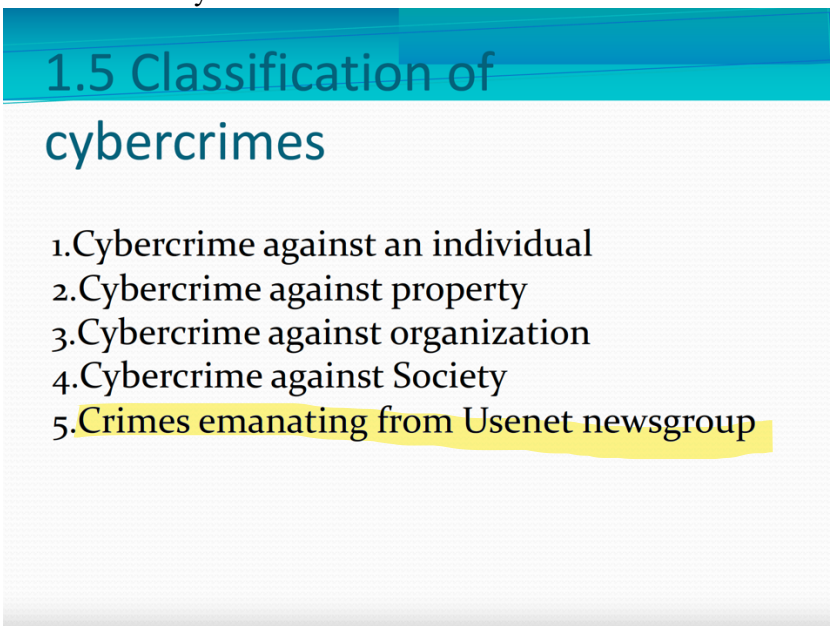
8. Explain the different Categories of Cybercriminals.







9. Explain the Classification of cybercrimes in detail.



1. Cybercrime against an individual

- Electronic mail spoofing and other online frauds
- Phishing, spear phishing
- spamming
- Cyberdefamation
- Cyberstalking and harassment
- Computer sabotage
- Pornographic offenses
- passwordsniffing

2.Cybercrime against property

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

3.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
- Industrial spying/ industrial espionage
- Computer network intrusions
- Software piracy

4.Cybercrime against Society

- Forgery
- Cyberterrorism
- Web jacking

5.Crimes emanating from Usenet newsgroup

- Usenet groups may carry very offensive, harmful, inaccurate material
- Postings that have been mislabeled or are deceptive in another way
- Hence service at your own risk

10. What are the main Motives behind cybercrime?

Motives behind cybercrime

- Greed
- Desire to gain power
- Publicity
- Desire for revenge
- A sense of adventure
- Looking for thrill to access forbidden information
- Destructive mindset
- Desire to sell network security services

11. Explain in detail about the Legal Perspectives, Global Perspective and Indian Perspective of Cybercrime.

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 - 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." -increasing number of transnational offenses.

•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).

  way is unrealistic

- The other is to incorporate the legal system into an integrated entity obliterating these state boundaries.

A Global Perspective on Cybercrimes

•***Australia,Cyber Crime Act 2001***, which details offenses against computer data and systems.

•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**.

•White-collar crime and economic crime.

•**International Telecommunication Union (ITU)** survey conducted in 2005.

- ITU activities on countering Spam can be read by visiting the link www.itu.int/spam (8 May 2010).
- The Spam legislation scenario mentions "none" about India as far as E-Mail legislation in India is concerned.
- The legislation refers to India as a "loose" legislation, although there is a mention in Section 67 of Indian ITA 2000.
- About 30 countries have enacted some form of anti-Spam legislation.

•No significant impact on the volume of Spam with spammers sending hundreds of millions of messages per day.

•The growing phenomenon is the use of Spam to support fraudulent and criminal activities – including attempts to capture financial information (e.g., account numbers and passwords) brand-spoofing" or "Phishing

•The extended enterprise can only be successful key.

•An extended enterprise is a "loosely coupled, self-organizing network" of firms that Combine their economic output to provide "products and services" offerings to the market.

•Firms in the extended enterprise may operate independently, for example, through market mechanisms or cooperatively through agreements and contracts.

•Vast flow of "information" to support instantaneous "decision-making ability" is crucial for the "external enterprise."

•This becomes possible through the "interconnected ness."

Cybercrimes: INDIAN Perspective

•India has the fourth highest number of Internet users in the world.

•India, 37% of all Internet accesses happen from cyber cafes 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, 50%crime increase in the year 2007.

•Hackers enders were under 30 years.

•The maximum cybercrime cases - cyber pornography,

•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.

12. What is the Survival Mantra for the Netizens.

Cybercrime Era: Survival Mantra for the Netizens

* The term "Netizen" are the Internet users.
* "Netizen" is someone **who spends considerable time online** and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms).

*The 5P Netizen mantra for online security is:

(a) Precaution,
(b) prevention,
(c) Protection,
(d) Preservation and
(e) Perseverance.

*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
- NASSCOM -- awareness is important; any matter should be reported at once.
- Cyberlabs across major cities in India
- Users must try and save any electronic information trail on their computers.
- That is all one can do until laws become more strength or technology more advanced.
- Some agencies have been advocating for the need to address protection of the Rights of Netizens.
- However, these NGOs efforts cannot provide complete support to the victims of cybercrimes
- Police have pursued false cases
- Agency to protect abuse of ITA 2000 in India was, therefore, a felt need for quite some time.

13. How Criminals Plan the cyber Attacks and explain the different phases of planning.

•How Criminals Plan the Attacks

•Criminals use many methods and tools to locate the vulnerabilities of their target.

•The target can be an individual and/or an organization.

•Criminals plan passive and active attacks

•**Active attacks** are usually used to alter the system (i.e., computer network) whereas **passive attacks** attempt to gain information about the target.

Phases are involved in planning cybercrime:

•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

•The literal meaning of "Reconnaissance" is *an act of* ***finding something or somebody*** (*especially to gain information about an enemy or potential enemy*).

•Phase begins with "*Foot printing*" – pre-attack phase, 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.

•This phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.

•Thus, an attacker attempts to gather information in two phases: passive and active attacks. Let us understand these two phases.

Passive Attacks

•A passive attack involves gathering information about a target without owners knowledge.

•simple as watching .

•Internet searches or by Googling (i.e., searching the required information with the help of search engine Google) an individual or company to gain information.

1.Google or Yahoo search: locate information about employees.

2.Surfing online community groups like Orkut/Facebook/instagram .

3.Organization's website may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target

4.Blogs, newsgroups, press releases, etc. are generally used as the mediums to gain information about the company or employees.

5.Going through the job postings.

Active Attacks

An active attack involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase.

•Risk of detection and is also called "Rattling the doorknobs" or "Active reconnaissance" , Attack.

Scanning and Scrutinizing Gathered Information

•Scanning is a key step to examine intelligently while gathering information about the target. The objectives of scanning are as follows:

1.Port scanning: Identify open/close ports and services.

2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.

3.Vulnerability scanning: Understand the existing weaknesses in the system.

Attack (Gaining and Maintaining the System Access)

•After the scanning and enumeration, the attack is launched using the following steps:

1.Crack the password.

2.exploit the privileges.

3.execute the malicious commands/applications.

4.hide the files (if required).

5.cover the tracks – delete the access logs, so that there is no trail illicit activity.

14. Explain in detail about social engineer and Social engineering.

Social Engineering

•Social engineering is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action.

•The natural tendency of a person to trust social engineers' word, rather than exploiting computer security holes.

•people are the weak in security and this principle makes social engineering possible.

•A social engineer usually uses telecommunication (i.e., telephone and/or cell phone) or Internet .

•Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.

•It is an art of exploiting the trust of people, which is not doubted while speaking in a normal manner.

•The goal of a social engineer is to fool someone into providing valuable information or access to that information.

•Social engineer studies the human behavior so that people will help because of the desire to be helpful, the attitude to trust people, and the fear of getting into trouble.

•The sign of truly successful social engineers is that they receive information without any suspicion.

Classification of Social Engineering

Human-Based Social Engineering
Computer-Based Social Engineering

Human-Based Social Engineering
person-to-person interaction to get the required/desired information.
An example is calling the help desk and trying to find out a password.

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
Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.
For example, sending a **fake E-Mail to the user** and asking him/her to re-enter a password in a webpage to confirm it.

Fake E-Mails
E-Mail attachments

Pop-up windows

15. Write a short note on Cyber stalking.

Cyberstalking

1. ***stalking*** -→Repeated and unwanted communications through phone calls, mail, or social media sites. Following the victim to work, school, home, or other places where they frequently visit. ... Repeatedly sending the victim unwanted gifts

2.The behavior includes : monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes

3.Cyber stalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to **harass another**

4.Cyber stalking refers to the use of Internet and/or other electronic communications devices to stalk another person.

5.It involves harassing or threatening behavior that an individual will conduct repeatedly

6. EXAMPLE

Types of Stalkers
There are primarily two types of stalkers.
Online stalkers
Offline stalkers:

Online stalkers:

1.start the interaction with the victim directly with the help of the Internet.
2.E-Mail and chat rooms are the most popular communication medium to get connected with the victim, rather than using traditional instrumentation like telephone/cell phone.
3.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:

1.attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
2.Searching on message boards/newsgroups, personal websites, and people finding services or websites are most common ways to gather information about the victim using the Internet.
3.The victim is not aware that the Internet has been used to perpetuate an attack against them.

Cases Reported on Cyberstalking

1.The majority of cyberstalkers are men and the majority of their victims are women.

2.Some cases also have been reported where vise versa , same—gender cyberstalking.

3.In many cases, the cyberstalker and the victim hold a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship, for example, ex-spouse, boss/subordinate, and neighbor.

4.However, there also have been many instances of cyberstalking by strangers.

How Stalking Works?

It is seen that stalking works in the following ways:

1.Personal information gathering about the victim: Name; family background; contact details such as cell phone and telephone numbers (of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.

2.Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.

3.cyber Stalkers will almost always establish a contact with the victims through E-Mail. 4.The stalker may use multiple names and ways while contacting the victim.

5.Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.

6.The stalker may post the victim's personal information on any website -- money

7.The stalker will use bad and/or offensive/attractive language to invite the interested persons.

16. Explain the relationship between Cyber cafe and Cybercrimes.

CyberCafe And CyberCrime

1.Café or coffee shop providing computers for access to the internet

2.Criminal activities carried out by means of computers or the internet.

3.Nielsen survey on the profile of cybercafes users in india,

- ✓ 90% of the audience, across eight cities
- ✓ 3,500 cafes
- ✓ male and in the age group of 15–35 years
- ✓ 52% were graduates and postgraduates
- ✓ almost over 50% were students.

4.Many instances have been reported in india, real or false terrorist communication.

5.Cybercafes -→ regularly for sending obscene mails to harass people.

6.Public computers, hold two types of risks.

•**First**, programs are installed on the computer – that is, risk of malicious programs such as *keyloggers* or *Spyware*

- •which maybe running at the background that can capture the keystrokes
  - •to know the passwords
  - •other confidential information
  - •monitor the browsing behavior.

•**Second**, over-the-shoulder surfing can enable others to find out your passwords.

- •Extremely careful about protecting his/her privacy on such systems
- •one does not know who will use the computer after him/her.

7. **Indian Information Technology Act (ITA) 2000,** does not define under the Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network.

8.Cybercriminals prefer cybercafes to carry out their activities.

9.The criminals tend to identify one particular personal computer (PC) to prepare it for their use.

10.Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.

11.Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.

12 . Security survey:

1.Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office).

2.Antivirus software is found to be not updated .

3.Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks.

4.Annual maintenance contract (AMC) found to be not in a place for servicing.

5.cybercriminal can install a Malicious Code on a computer and conduct criminal activities without any interruption.

17. Write a short note on Botnets.

Botnets: The Fuel for Cybercrime

Botnet

•Bot is *an automated program for doing some particular task, over a network.*,

•Collection of software robots, or bots

• Run automatically.

•Under the control of a remote attacker.

•Malicious software but can also refer to the network of computers using distributed computing software.

•A bot is simply an automated computer program one can gain the control of computer by infecting them with a virus or other malicious code that gives the access.

•Computer system maybe a part of a botnet even though it appears to be operating normally.

•Botnets are often used to conduct a range of activities, from distributing spam and viruses to conducting denial-of-service (dos) attacks

•A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.

•"*Zombie networks*" have become a source of income for entire groups of cybercriminals.

18. Write a short note on Attack Vector.

Attack Vector

•**An "attack vector" is a path**, which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.

•exploit system vulnerabilities, including the human element.

•**Attack vectors** include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms.

• methods involve programming ,human operator is fooled into removing or weakening system defenses.

•To some extent, firewalls and antivirus software can block attack vectors.

•However, no protection method is totally attack-proof.

•A defense method that is effective today may not remain so for → updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers.

•common malicious viruses, Trojan Horses, worms, and Spyware.

•If an attack vector as guided missile ---- dest

•In the*payload* is the necessary data being carried within a packet or other transmission

• payload does not include the "overhead" data required to get the packet to its destination

•Payload may depend on the following point of view

•payload is sometimes considered to include that part of the overhead data that this layer handles --- >hackers called attack vector

The attack vectors described here are how most of them are launched.

1.Attack by E-Mail

2.Attachments (and other files)

3.Attack by deception

4.Hackers: as owners

5.Heedless guests (attack by webpage

6.Attack of the worms &logical worms

7.Malicious macros

8.Foistware (sneakware)

9.Viruses

19. Explain in detail about Cloud Computing and how to protect data in the cloud.

Cloud Computing

•growing popularity of cloud computing and virtualization -- next target of cybercriminals.

•Cloud computing services,

- considerable benefits data travel
- cost savings,
- move servers outside the organizations security perimeter,

which make it easier for cybercriminals to attack these systems.

•The term cloud is used as a metaphor for the Internet, based on the cloud drawing used to depict the Internet in computer networks.

•Cloud computing is a term used for hosted services delivered over the Internet.

•A cloud service has three distinct characteristics :

- It is sold on demand
- It is elastic in terms of usage
- The service is fully managed by the provider – a user just needs PC and Internet connection.

Why Cloud Computing?

•Applications and data can be accessed from anywhere at any time.

•Data may not be held on a hard drive on one user's computer.

•It could bring hardware costs down. One would need the Internet connection.

•Organizations do not have to buy a set of software or software licenses for every employee

•Organizations do not have to rent a physical space to store servers and databases

•Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware.

•The cloud computing services can be either private or public.

Types of Services

•Infrastructure-as-a-service (IaaS):

- **blocks of storage** on demand.
- pay for exactly the amount of service they use, like for electricity or water, this service is also called utility computing.

•Platform-as-a-service (PaaS):

- set of software and development tools hosted on the provider's servers.
- Developers can create applications using the provider's APIs. **Google Apps**

▪Software-as-a-service (SaaS)

- ▪the provider allows the customer only to use its applications. E-Mail ,Twitter

Precautions to protect and keep your data safe on the cloud.

•Use a Password Manager

•Embrace Two-Factor Authentication

•Adapt the Principle of Least Privilege

•Control Access for Third-Party Apps

•Arm Yourself with Knowledge

- **Verify ,Ignore ,Do not open**

•Back Up Cloud Data

•Data Backup Strategies