IOMoARcPSD|26360945

1. INTRODUCTION TO CYBERCRIME

List of Topics:

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

INTRODUCTION

- **"**Cyber security is the protection of internet-connected systems, including hardware, software and data, from cyber attacks**"**.
- Almost everyone is aware of the rapid growth of the Internet.
- Given the unrestricted number of free websites, the Internet has undeniably opened a new way of exploitation known as cybercrime.
- These activities involve the use of computers, the Internet, cyberspace and the worldwide web (WWW).
- Interestingly, cybercrime is not a new phenomena; the first recorded cybercrime took place in the year 1820.
- It is one of the most talked about topics in the recent years.
- Based on a 2008 survey in Australia, the below shows the cybercrime trend

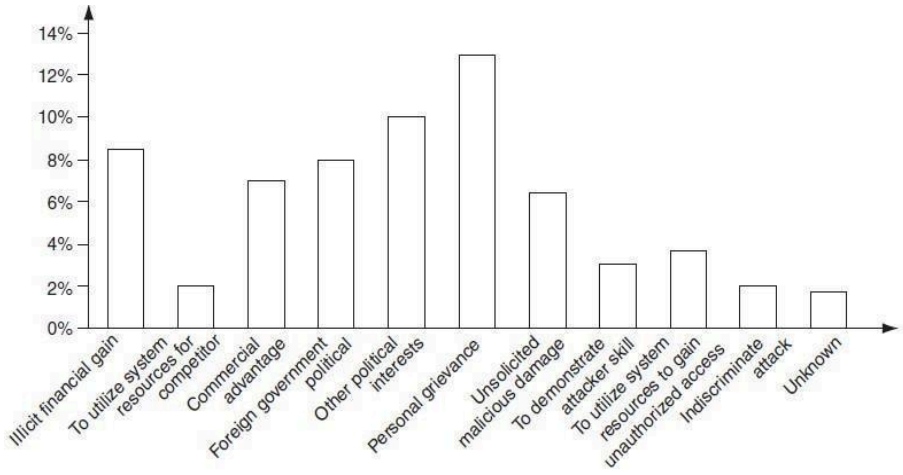


Figure: Cybercrime Trend

- Indian corporate and government sites have been attacked or defaced more than 780 times between February 2000 and December 2002.
- There are also stories/news of other attacks; for example, according to a story posted on 3 December 2009, a total of 3,286 Indian websites were hacked in 5 months – between January and June 2009.
- Various cybercrimes and cases registered under cybercrimes by motives and suspects in States and Union Territories (UTs).

CYBERCRIME: DEFINITION AND ORIGINS OF THE WORD

Definition:

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

Alternative definitions of Cybercrime are as follows:

1. Any illegal act where a special knowledge of computer technology is essential for its perpetration (to commit a crime), investigation or prosecution.
2. Any financial dishonesty that takes place in a computer environment.
3. Any threats to the computer itself, such as theft of hardware or software, damage and demands for money.
4. "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."

The term "cybercrime" relates to a number of other terms that may sometimes be used to describe crimes committed using computers. • Computer-related crime

- Computer crime
- Internet crime
- E-crime
- High-tech crime, etc. are the other synonymous terms.

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

1. **Techno-crime:** A premeditated act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system. The 24X7 connection to the internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, if any, "finger prints".
2. **Techno-vandalism:** These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature. Tight internal security, allied to strong technical safeguards should prevent the vast majority of such incidents.

There is a very thin line between the two terms "computer crime" and "computer fraud"; both are punishable. Cybercrimes (harmful acts committed from or against a computer or network) differ from most terrestrial crimes in four ways:

a. how to commit them is easier to learn,
b. they require few resources relative to the potential damage caused,
c. they can be committed in a jurisdiction without being physically present in it & d. they are often not clearly illegal.

Important Definitions related to Cyber Security:

Cyberterrorism:

This term was coined in 1997 by Barry Collin, a senior research fellow at the institute for Security and Intelligence in California. Cyberterrorism is defined as "any person, group or organization who, with terrorist intent, utilizes accesses or aids in accessing a computer or computer network or electronic system or electronic device by any available means, and thereby knowingly engages in or attempts to engage in a terrorist act commits the offence of cyberterrorism."

Cybernetics:

Cybernetics is an interdisciplinary field that explores the principles of control and communication in systems, whether they are biological, mechanical, social, or computational. It involves analyzing feedback loops, information processing, and regulatory mechanisms to understand how systems function, learn, and evolve. By studying cybernetics, we gain insights into the dynamics of complex systems and develop strategies for effective control, optimization, and decision-making in various domains..

Phishing:

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

(or)

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

Cyberspace:

This is a term coined by William Gibson, a science fiction writer in 1984. The term "cyberspace" is now used to describe the Internet and other computer networks. In terms of computer science, "cyberspace" is a worldwide network of computer networks that uses the Transmission Control Protocol/Internet Protocol (TCP/IP) for communication to facilitate transmission and exchange of data. Cyberspace is most definitely a place where you chat, explore, research and play.

Cybersquatting:

Cybersquatting is when someone registers or uses a domain name that is similar to a well-known brand or trademark, with the intention of profiting from it or causing harm to the brand.

Cyberpunk:

This is a term coined by Bruce Bethke, published in science fiction stories magazine in November 1983. According to science fiction literature, the words "cyber" and "punk" emphasize the two basic aspects of cyberpunk: "technology" and "individualism." The term "cyberpunk" could mean something like "anarchy via machines" or "machine/computer rebel movement."

Cyberwarfare:

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

The Botnet Menace: The botnet menace refers to the significant threat posed by botnets in the realm of cybersecurity. A botnet is a network of compromised computers or devices that are under the control of a central command-and-control (C&C) infrastructure operated by cybercriminals. These compromised devices, often referred to as "bots" or "zombies," are typically infected with malware without the knowledge or consent of their owners.

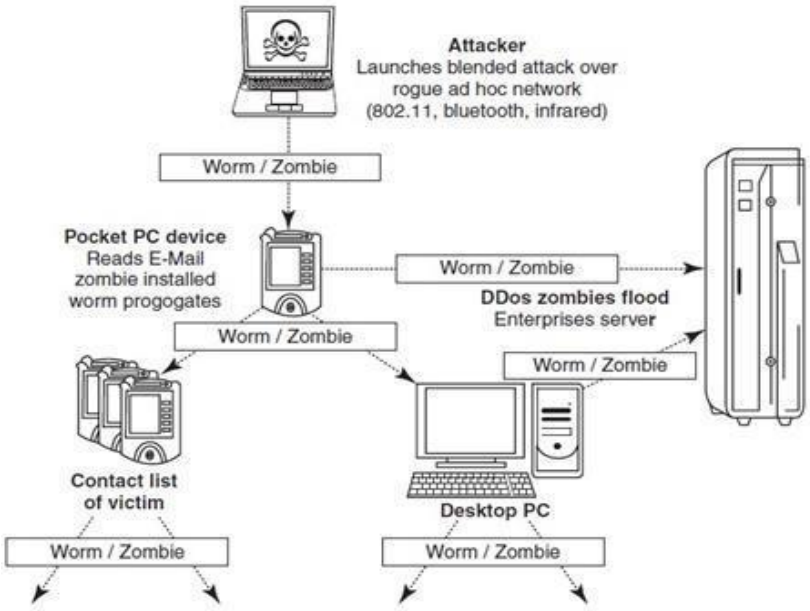


Figure: How a Zombie works

The botnet menace refers to the significant threat posed by botnets in the realm of cybersecurity. A botnet is a network of compromised computers or devices that are under the control of a central command-and-control (C&C) infrastructure operated by cybercriminals. These compromised devices, often referred to as "bots" or "zombies," are typically infected with malware without the knowledge or consent of their owners.

The botnet menace arises from the malicious activities that botnets can engage in, including:

1. **Distributed Denial of Service (DDoS) Attacks:** Botnets can be used to launch large-scale DDoS attacks, where a massive amount of traffic is directed towards a target system or website, overwhelming it and causing disruption or downtime.

2. **Spam Distribution**: Botnets can be used to distribute spam emails in large volumes, contributing to the proliferation of unwanted and potentially malicious messages.

3. **Information Theft:** Botnets may be used to harvest sensitive information, such as login credentials, financial data, or personal information, from compromised devices, leading to identity theft or financial loss.

4. **Cryptocurrency Mining:** Cybercriminals can utilize botnets for cryptocurrency mining, hijacking the computational resources of infected devices to mine cryptocurrencies without the owner's consent or knowledge.

5. **Malware Distribution:** Botnets can be used as a platform for distributing malware, spreading infections to other vulnerable devices and expanding the botnet's size and capabilities.

WHO ARE CYBERCRIMINALS?

Cybercrime involves such activities

- credit card fraud;
- cyberstalking;
- defaming another online;
- gaining unauthorized access to computer systems;
- ignoring copyright, software licensing and trademark protection;
- overriding encryption to make illegal copies;
- software piracy and stealing another's identity (known as identity theft) to perform criminal acts

Types of Cybercriminals:

1. **Type I: Cybercriminals – hungry for recognition**
    - Hobby hackers;
    - IT professionals (social engineering is one of the biggest threat);
    - Politically motivated hackers;
    - Terrorist organizations.
2. **Type II: Cybercriminals – not interested in recognition**
    - Psychological perverts;
    - financially motivated hackers (corporate espionage);
    - state-sponsored hacking (national espionage, sabotage)
    - organized criminals
3. **Type III: Cybercriminals – the insiders**
    - Disgruntled or former employees seeking revenge;
    - Competing companies using employees to gain economic advantage through damage and/or theft.

CLASSIFICATIONS OF CYBERCRIMES

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

Table: Classifying Cybercrimes

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

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

Cybercrime against individual

1. **E-Mail Spoofing:** A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source. For example, let us say, Roopa has an E-Mail address roopa@asianlaws.org. Let us say her boyfriend Suresh and she happen to have a show down. Then Suresh, having become her enemy, spoofs her E-Mail and sends vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from Roopa, her friends could take offense and relationships could be spoiled for life.
2. **Online Frauds:** The most common types of online fraud are called phishing and spoofing. Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, etc. Often times the e-mails directs you to a website where you can update your personal information. Because these sites often look "official," they hope you'll be tricked into disclosing valuable information that you normally would not reveal. This often times, results in identity theft and financial loss.

Types of phishing

Vishing :Vishing, short for "voice phishing," is a form of social engineering attack that takes place over phone calls. It involves an attacker impersonating a trusted entity, such as a bank representative, government agency, or technical support personnel, in order to deceive individuals into sharing sensitive information or performing certain actions.

During a vishing attack, the attacker may use various tactics to gain the target's trust and manipulate them into divulging personal information, such as bank account details, social security numbers, or passwords. They may create a sense of urgency or fear, making the target believe that immediate action is required to prevent negative consequences.

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

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

4. **Spamming:** Spamming refers to the act of sending unsolicited or unwanted messages or content in bulk through electronic communication channels, primarily email. It involves the mass distribution of messages, often advertisements or promotional material, to a large number of recipients who have not consented to receive such communications. Spamming is typically done for commercial purposes, aiming to promote products or services, but it can also include malicious content or scams. Spamming can be disruptive, annoying, and can overload email systems or other messaging platforms.

5. **Cyber defamation** Cyber defamation, also known as online defamation, refers to the act of making false and damaging statements about someone on the internet. It involves posting or sharing false information or statements that harm a person's reputation or character through online platforms such as social media, blogs, forums, or websites. Cyber defamation can cause significant harm to an individual's personal or professional life, and it is considered a form of online harassment**.**

6. **Cyberstalking and harassment:** Cyberstalking is when someone uses the internet or electronic communication platforms to repeatedly and intentionally harass, threaten, or intimidate another person. It involves persistently engaging in unwanted behavior, such as sending threatening messages, monitoring the

victim's online activities, or spreading false information about them. Cyberstalking can cause fear, distress, or emotional harm to the victim and is considered a serious form of online harassment.

7. **Pornographic Offenses:** Pornographic offenses refer to illegal activities involving explicit sexual material. This can include creating, distributing, or possessing pornography that may involve minors, be considered offensive or lacking value, or involve non-consensual acts. Revenge porn, which involves sharing intimate images without consent, is also considered a pornographic offense. Laws and punishments vary by jurisdiction. It is important to respect the laws and consent of individuals involved.

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

And yet, password sniffers aren't always used for malicious intent. They are often used by IT professionals as a tool to identify weak applications that may be passing critical information unencrypted over the Local Area Network (LAN).

Cybercrime against property

1. **Credit Card Frauds:** Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help businesses process card payments securely and reduce card fraud. Credit card fraud can be authorised, where the genuine customer themselves processes a payment to another account which is controlled by a criminal, or unauthorised, where the account holder does not provide authorisation for the payment to proceed and the transaction is carried out by a third party.
2. **Intellectual Property (IP) Crimes:** With the growth in the use of internet these days the cyber crimes are also growing. Cyber theft of Intellectual Property (IP) is one of them. Cyber theft of IP means stealing of copyrights, software piracy, trade secrets, patents etc., using internet and computers.

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

- **Internet time theft:** Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person. Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent. The issue of Internet time theft is related to the crimes conducted through identity theft.

Cybercrime against Organization

1. **Unauthorized accessing of Computer:** Hacking is one method of doing this and hacking is punishable offense. Unauthorized computer access, popularly referred to as hacking, describes a criminal action whereby someone uses a computer to knowingly gain access to data in a system without permission to access that data.
2. **Denial-of-service Attacks (DoS Attacks):** A DoS attack is when someone deliberately overloads a computer network, website, or online service with too much data or requests. This makes the system unable to respond to legitimate users, causing disruptions or even complete shutdowns. The goal is to disrupt the targeted system and cause inconvenience or damage.
3. **Virus attacks/dissemination of Viruses:**

   A virus attack occurs when harmful software, called a computer virus, infects a computer or network. The virus is designed to cause damage, steal information, or disrupt the normal operation of the system. It spreads by tricking users into downloading infected files or programs. Once inside, the virus can replicate itself, corrupt files, steal data, or harm the computer's overall functionality. To protect against virus attacks, it is important to use antivirus software, update systems regularly, and be cautious when downloading files or visiting websites.
4. **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 or to make victim's mail servers crash .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.

5. **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.

6. **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.

7. **Software piracy:**

   Software piracy refers to the unauthorized copying, distribution, or use of software without the permission of the copyright owner. It involves obtaining and using software in violation of the terms and conditions set by the software license.

   Software piracy can take various forms, including:

   1. **Copying:** Making unauthorized copies of software and distributing them to others without the proper license or permission.

   2. **Downloading:** Obtaining software from unauthorized sources, such as torrent websites or file-sharing networks, without paying for it or following the licensing requirements.

   3**. Sharing:** Distributing software among multiple users or organizations without the appropriate licenses or permissions.

   4. **Counterfeiting:** Producing and selling counterfeit copies of software, making it appear genuine while infringing on the copyrights of the original software.

   To avoid software piracy, it is important to respect software copyrights, purchase legitimate copies, and comply with software licensing agreements. Using open-source software or free software provided under appropriate licenses is also a legal and ethical alternative.

Cybercrime against Society

1. **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.

2. **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.

3. **Web Jacking:** Web jacking occurs when someone forcefully takes control of a website (by cracking the password and later changing it). Thus, the first stage of this crime involves "password sniffing". The actual owner of the website does not have any more control over what appears on that website.

Crimes emanating from Usenet newsgroup:

By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way. Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.

Usenet is a popular means of sharing and distributing information on the Web with respect to specific topic or subjects. Usenet is a mechanism that allows sharing information in a many-to-many manner. The newsgroups are spread across 30,000 different topics.

CYBERCRIME & THE INDIAN ITA 2000

In India, the ITA 2000 was enacted after the United Nation General Assembly Resolution A/RES/51/162 in January 30, 1997 by adopting the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law. This was the first step toward the Law relating to ECommerce 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:

S

Section Ref. and Title	Chapter of the Act And Title	Crime	Punishment
Sec.43 (Penalty for damage to computer, computer system etc)	Chapter IX Penalties and Adjudication	Damage to computer system etc.	Compensation for Rs. 1 Crore
Sec.66 (Hacking with computer system)	Chapter XI Offences	Hacking (with intent or knowledge)	Fine of Rs. 2 Lakhs & Imprisonment for 3 year
Sec.67 (Publishing of information which is obscene in electronic form)	Chapter XI Offences	Publication of obscene material in electronic form	Fine of Rs. 1 Lakh & Imprisonment of 5 years and double conviction on second offence
Sec.68 (Power of controller to give directions)	Chapter XI Offences	Not complying with directions of controller	Fine upto Rs. 2 Lakhs & Imprisonment of 3 years
Sec.70 (Protected System)	Chapter XI Offences	Attempting or securing access to computer of another person without his/her knowledge	Imprisonment up to 10 Years
Sec.72 (Penalty for breach of confidentiality	Chapter XI Offences	Attempting or securing access to computer for	Fine up to Rs. 1 Lakh and Imprisonment up to
and privacy)		breaking confidentiality of the information of computer	2 Years
Sec.73 (Penalty for publishing Digital Signature Certificate false in certain particulars)	Chapter XI Offences	Publishing false Digital Signatures, false in certain particulars	Fine of Rs.1 Lakh or imprisonment of 2 years or both
Sec.74 (Publication for fraudulent purpose)	Chapter XI Offences	Publishing of Digital Signatures for fraudulent purpose	Imprisonment for the term of 2 years and fine of Rs. 1 Lakh

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

A GLOBAL PERSPECTIVE ON CYBERCRIMES

The linkage of cybersecurity and critical infrastructure protection has become a big issue as a number of countries have began assessment of threats, vulnerabilities and started exploring mechanisms to redress them. Recently, there have been a number of significant developments such as

1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime. The convention targets hackers, those spreading destructive computer viruses, those using the Internet for the sexual exploitation of children or the distribution of racist material, and terrorists attempting to attack infrastructure facilities or financial institutions. The Convention is in full accord with all the US constitutional protections, such as free speech and other civil liberties, and will require no change to the US laws.
2. In August 18, 2006, there was a news article published "ISPs Wary About 'Drastic Obligations' on Web Site Blocking." European Union (EU) officials want to debar suspicious websites as part of a 6-point plan to boost joint antiterrorism activities. They want to block websites that incite terrorist action. Once again it is underlined that monitoring calls, Internet and E-Mail traffic for law enforcement purposes is a task vested in the government, which must reimburse carriers and providers for retaining the data.
3. CoE Cyber Crime Convention (1997–2001) was the first international treaty seeking to address Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. More than 40 countries have ratified the Convention to date.

Cybercrime and the Extended Enterprise:

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

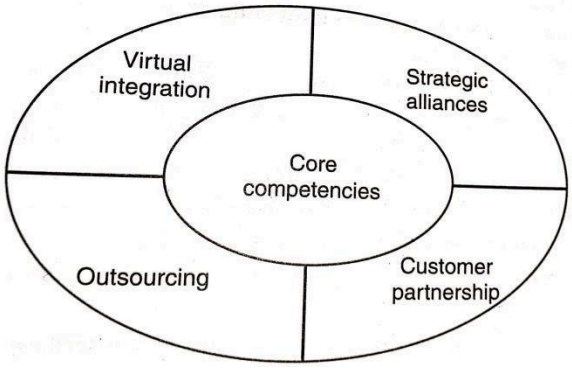


Figure: Extended Enterprise

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

CYBERCRIME ERA: SURVIVAL MANTRA FOR THE NETIZENS

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

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

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

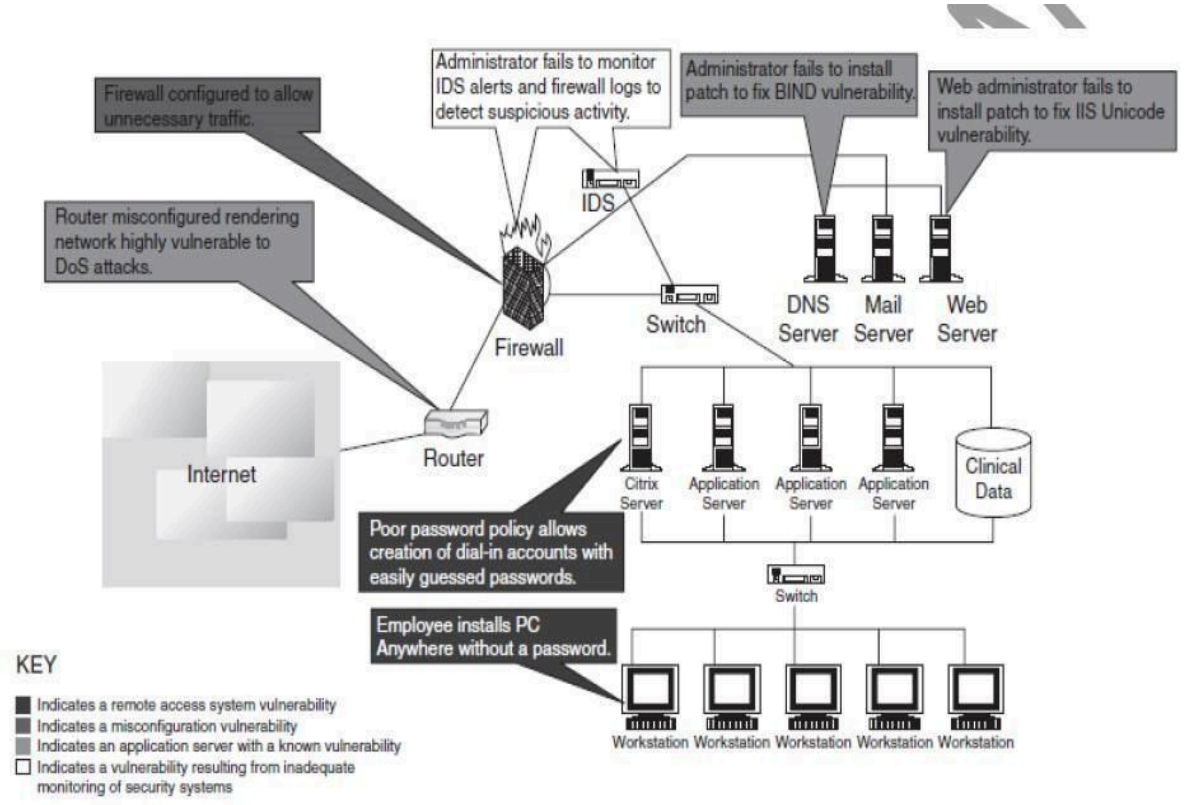
More importantly, users must try and save any electronic information trail on their computers. That is all one can do until laws become more stringent or technology more advanced. Some agencies have been advocating for the need to address protection of the Rights of Netizens. There are agencies that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

How Criminals Plan Them –Introduction

- Technology is a "double-edged sword" as it can be used for both good and bad purposes

- People with the tendency to cause damages or carrying out illegal activities will use it for bad purpose.
- Computers and tools available in IT are also used as either target of offense.
- In today's world of Internet and computer networks, a criminal activity can be carried out across national borders.
- Chapter 1 provided an overview of hacking, cyber terrorism, network intrusions, password sniffing, computer viruses, etc. They are the most commonly occurring crimes that target the computer.
- Cybercriminal use the World Wide Web and Internet to an optimum level for all illegal activities to store data, contacts, account information, etc.
- The criminals take advantage of the widespread lack of awareness about cybercrimes and cyber laws among the people who are constantly using the IT infrastructure for official and personal purposes.
- People who commit cybercrimes are known as "Crackers" (Box 2.1).

Box 2.1 | Hackers, Crackers and Phreakers
Hacker: A hacker is a person with a strong interest in computers who enjoys learning and experimenting with them. Hackers are usually very talented, smart people who understand computers better than others. The term is often confused with cracker that defines someone who breaks into computers (refer to Box 2.2).
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. Crackers should not be confused with hackers. The term "cracker" is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas.
Cracking: It is the act of breaking into computers. Cracking is a popular, growing subject on the Internet. Many sites are devoted to supplying crackers with programs that allow them to crack computers. Some of these programs contain dictionaries for guessing passwords. Others are used to break into phone lines (called "phreaking"). These sites usually display warnings such as "These files are illegal; we are not responsible for what you do with them."
Cracker tools: These are programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war dialers and worms.
Phreaking: This is the notorious art of breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals.
War dialer: Program automatically dials phone numbers looking for computers on the other end. It catalogs numbers so that the hackers can call back and try to break in. An attacker would look to exploit the vulnerabilities in the networks, most often so because the networks are not adequately protected.



- The categories of vulnerabilities that hackers typically search for are the following:
  - Inadequate border protection (border as in the sense of network periphery); ○ remote access servers (RASs) with weak access controls;
  - application servers with well-known exploits; ○ misconfigured systems and systems with default configurations.
- To help the reader understand the network attack scenario, Fig. 2.2 illustrates a small network highlighting specific occurrences of several vulnerabilities described above.

Box 2.2 | What Color is Your Hat in the Security World?

A **black hat** is also called a "cracker" or "dark side hacker." Such a person is a malicious or **criminal hacker**. Typically, the term "cracker" is used within the security industry. However, the general public uses the term hacker to refer to the same thing. In computer terminology, the meaning of "hacker" can be much broader. The name comes from the opposite of "white hat hackers."

A **white hat hacker** is considered an **ethical hacker**. In the realm of IT, a "white hat hacker" is a person who is ethically opposed to the abuse of computer systems. It is said that the term is derived from American western movies, where the protagonist typically wore a white cowboy hat and the antagonist typically wore a black one. As a simplified explanation, a "white hat" generally focuses on securing IT systems, whereas a "black hat" (the opposite) would like to break into them, so this sounds like an age-old game of a thief and a police.

A **brown hat hacker** is one who thinks before acting or committing a malice or non-malice deed. A grey hat commonly refers to a hacker who releases information about any exploits or security holes he/she finds openly to the public. He/she does so without concern for how the information is used in the end (whether for patching or exploiting).

2.1.1 Categories of Cybercrime

Cybercrime can be categorized based on the following:

1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

Cybercrime can be targeted against individuals (**persons**), assets (**property**) and/or **organizations** (government, business and social).

1. **Crimes targeted at individuals:** The goal is to exploit human weakness such as greed and naivety. These crimes include financial frauds, sale of non-existent or stolen items, child pornography (explained in Section 1.5.13, Chapter 1), copyright violation, harassment, etc. 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. However, this also makes difficult to trace and apprehend the criminals.
2. **Crimes targeted at property:** This includes stealing mobile devices such as cell phone, laptops, personal digital assistant (PDAs), and removable medias (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, etc.
3. **Crimes targeted at organizations:** Cyber terrorism is one of the distinct crimes against organizations/ governments. Attackers (individuals or groups of individuals) use computer tools and the Internet to usually terrorize the citizens of a particular country by stealing the private information, and also to damage the programs and fi les or plant programs to get control of the network and/or system (see Box 2.3).
4. **Single event of cybercrime:** It is the single event from the perspective of the victim. For example, unknowingly open an attachment that may contain virus that will infect the system (PC/laptop). This is known as hacking or fraud.
5. **Series of events:** This involves attacker interacting with the victims repetitively. For example, 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.

2.2 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.
- **Active attacks** may affect the availability, integrity and authenticity of data whereas **passive attacks** lead to violation of confidentiality.

The following phases are involved in planning cybercrime:

1. Reconnaissance (information gathering) is the first phase and is treated as **passive attacks.**

2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

2.2.1 Reconnaissance (reconnaissance= ಪದ)

- The literal meaning of "Reconnaissance" is an act of **finding something or somebody**

Reconnaissance, in the context of cybersecurity, refers to the phase of gathering information and intelligence about a target system, network, or organization. It is the initial step that attackers take to understand the target's vulnerabilities, potential entry points, and security measures in place. Reconnaissance can be conducted actively or passively, and it helps attackers plan and execute their subsequent attacks effectively.

There are two primary types of reconnaissance in cybersecurity:

1. **Active Reconnaissance:** Active reconnaissance involves direct interaction with the target system or network. It typically includes techniques such as port scanning, network scanning, vulnerability scanning, and enumeration. The goal is to identify open ports, available services, system configurations, and potential weaknesses that can be exploited.
2. **Passive Reconnaissance**: Passive reconnaissance focuses on gathering information about the target without direct interaction. It involves monitoring publicly available sources, such as websites, social media, online forums, or public databases, to collect data about the target's infrastructure, employees, business partners, or technology stack. This information can provide insights into the target's security posture and potential vulnerabilities.

. **2.2.2 Passive Attacks**

A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge. It can be as simple as watching a building to identify what time employees enter the building premises. However, it is usually done using 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: People search to locate information about employees.
2. Surfing online community groups like Orkut/Facebook will prove useful to gain the information about an individual.
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 (see Section 2.3).
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 in particular job profiles for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

2.2.3 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. It involves the risk of detection and is also called "Rattling the doorknobs" or "Active reconnaissance." Active

reconnaissance can provide confirmation to an attacker about security measures in place (e.g., whether the front door is locked?), but the process can also increase the chance of being caught or raise a suspicion.

2.2.4 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. Refer to Box 2.5.
2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.
3. **Vulnerability scanning:** Understand the existing weaknesses in the system.

2.2.5 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.

2.3 Social Engineering

Social engineering is a technique used by cyber attackers to manipulate individuals into revealing sensitive information, performing certain actions, or bypassing security measures. It involves psychological manipulation rather than technical exploits to deceive and trick people into providing access to confidential data, systems, or networks.

Social engineering attacks exploit human vulnerabilities and tendencies, such as trust, curiosity, fear, or the desire to help others. Attackers often impersonate someone trustworthy or authoritative, such as a colleague, technical support personnel, or a reputable organization, to gain the target's confidence.

2.3.1 Classification of Social Engineering

Human-Based Social Engineering

- Human-based social engineering refers to person-to-person interaction to get the required/desired information.
- An example is calling the help desk and trying to find out a password.

1. Impersonating an employee or valid user:

- “Impersonation” is perhaps the greatest technique used by social engineers to deceive people.
- Social engineers “take advantage” of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who “forgot” his/her badge, etc., or pretending to be an employee or valid user on the system.

2. Posing as an important user:

- The attacker pretends to be an important user – for example, a Chief Executive Officer (CEO) or high-level manager who needs immediate assistance to gain access to a system.
- The attacker uses intimidation so that a lower-level employee such as a help-desk worker will help him/her in gaining access to the system. Most of the low-level employees will not ask any question to someone who appears to be in a position of authority.

3. Using a third person:

- An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.

4. Calling technical support:

- Calling the technical support for assistance is a classic social engineering example.
- Help-desk and technical support personnel are trained to help users, which makes them good prey for social engineering attacks.

5. Shoulder surfing:

- It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.

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.

1.Fake E-Mails:

commonly known as phishing emails, are deceptive electronic messages sent by cyber attackers to trick recipients into divulging sensitive information, performing actions, or downloading malicious content. These emails are designed to appear legitimate and often impersonate well-known organizations, financial institutions, or trusted individuals.

1. E-Mail attachments:

- E-Mail attachments are used to send malicious code to a victim's system, which will automatically (e.g., keylogger utility to capture passwords) get executed.
- Viruses, Trojans, and worms can be included cleverly into the attachments to entice a victim to open the attachment.

2. Pop-up windows:

- Pop-up windows are also used, in a similar manner to E-Mail attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

2.4 Cyberstalking

- The dictionary meaning of "stalking" is an "act or process of following prey stealthily – trying to approach somebody or something."
- Cyberstalking has been defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to **harass another individual, group of individuals, or organization**.
- The behavior includes false accusations, monitoring, transmission of threats, ID theft, damage to data or equipment, solicitation of minors for sexual purposes, and gathering information for harassment purposes.
- Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person.

- **It 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, or vandalizing against the person's property. As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

2.4.1 Types of Stalkers

There are primarily two types of stalkers.

1. **Online stalkers:**
   - They aim to start the interaction with the victim directly with the help of the Internet.
   - 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.
   - 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.
2. **Offline stalkers:**
   - The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.
   - 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.
   - The victim is not aware that the Internet has been used to perpetuate an attack against them.

2.4.2 Cases Reported on Cyberstalking

- The majority of cyberstalkers are men and the majority of their victims are women.
- Some cases also have been reported where women act as cyberstalkers and men as the victims as well as cases of same-sex cyberstalking.
- 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-lover, ex-spouse, boss/subordinate, and neighbor.
- However, there also have been many instances of cyberstalking by strangers.

2.5 Cybercafe and Cybercrimes

A cybercafe is a location that provides internet access to the public for a fee. It typically offers computer terminals or Wi-Fi connectivity for individuals to use for various online activities.

- Cybercrimes, on the other hand, refer to criminal activities that are committed using computer networks or the internet. These crimes can include a wide range of illegal activities, such as hacking, identity theft, phishing, online fraud, cyberbullying, unauthorized access to systems, distribution of malicious software, and online harassment, among others.
- Cybercafes can inadvertently become a breeding ground for cybercrimes if not properly regulated or monitored. Due to the open and public nature of cybercafes, individuals with malicious intent may use the provided internet access to engage in illegal activities, potentially causing harm to others or compromising the security of systems and networks.

- To mitigate the risk of cybercrimes in cybercafes, it is essential for operators to implement security measures, such as ensuring secure network infrastructure, monitoring user activities, and educating customers about safe and responsible online behavior. Cooperation with law enforcement agencies and adherence to legal and regulatory requirements is also crucial in preventing cybercrimes in such establishments. In the event that a central agency takes up the responsibility for monitoring cybercafes, an individual should take care while visiting and/or operating from cybercafe.

Here are a few tips for safety and security while using the computer in a cybercafe:

1. **Always logout:**
2. **Stay with the computer:**
3. **Clear history and temporary files:**
4. **Be alert:**
5. **Avoid online financial transactions:**
6. **Change passwords:**
7. **Use Virtual keyboard:**
8. **Security warnings:**

2.6 Botnets: The Fuel for Cybercrime

2.6.1 Botnet

A botnet is called as a collection of infected devices which are internet connected and these devices are controlled by the cyber-criminal with the help of malware. Usually, users are unaware of a botnet that is affecting their PC. Botnets normally used to send spam mails, create unusual traffic, etc.

Botnet is installed on the PC which is vulnerable because of outdated firewalls or antivirus.

Once the target device gets affected the attacker can control bots with two approaches –

- **Client server approach** – In this approach, first a server is set up which then sends commands to bots via communication protocol. After getting the command bots do the corresponding malicious activity.
- **Peer to peer approach** – This is a decentralized approach in which there is no main server. This approach is very common nowadays because Cyber security is still using the C&C communication to search for these malicious activities. In this approach Infected devices search for the infected website or devices in the same bot. Then they share the updated command of the botnet malware.

Defender can easily find the botnet malware because most of them are still using a centralized approach so it becomes an advantage for the defender.

For example – Zeus malware uses Trojan horse to infect the vulnerable devices. In 2009 cyber security found that 3.6 million hosts were infected by this malware.

Botnet is one of the examples which use good technologies for bad intentions. The most common uses that are criminally motivated for the following purposes –

- Distributed denial of service attacks
- Spamming
- Sniffing Traffic
- Key logging
- Spreading new malware
- Google AdSense abuse
- Attacking chat networks
- Mass identity theft

Uses

The uses of botnets are as follows –

- These are used for Distributed Denial of Service attacks
- These are used by the cyber criminals to investigate Botnet attacks such as unauthorized access, data leakage and credential leakage, data theft etc.

Botnet attack to wireless devices

Botnets are not made to trade off only one individual computer; they are intended to contaminate a large number of remote devices. Bot herders regularly send botnets onto computers through a trojan stallion virus.

The procedure regularly expects clients to contaminate their own particular frameworks by opening email connections, tapping on malicious fly up advertisements, or downloading hazardous software from a site.

In the wake of contaminating devices, botnets are unable to get to and adjust individual data, attack different computers, and perpetrate different wrongdoings.

More mind boggling botnets can even self-engender finding and tainting devices naturally. Such self-governing bots do look for-and-contaminate missions, always scanning the web for defenseless web-associated devices lacking working framework refreshes or antivirus software.

2.7 Attack Vector

In the context of cybersecurity, an attack vector refers to the method or pathway through which an attacker gains unauthorized access to a computer system, network, or application in order to compromise its security. It represents the specific vulnerability or weakness that an attacker exploits to carry out their malicious activities.

Attack vectors can take various forms and exploit different types of vulnerabilities, including:

1. Phishing and Social Engineering: These attacks involve tricking individuals into revealing sensitive information or performing certain actions by impersonating trusted entities through deceptive emails, messages, or phone calls.

2. Malware: Attackers may use malicious software, such as viruses, worms, Trojans, or ransomware, to infect systems and gain control over them, steal data, or cause disruptions.

3. Exploiting Software Vulnerabilities: Attackers search for and exploit vulnerabilities or weaknesses in software applications, operating systems, or network infrastructure to gain unauthorized access or control over targeted systems.

4. Brute Force Attacks: These involve systematically trying all possible combinations of passwords or encryption keys to gain unauthorized access to a system or network.

5. Distributed Denial-of-Service (DDoS) Attacks: Attackers overwhelm a targeted system or network with a massive volume of traffic or requests, rendering it unable to function properly and denying access to legitimate users.

6. Insider Threats: Attacks may be carried out by individuals who have authorized access to the system or network but abuse their privileges or share sensitive information with malicious intent.

Understanding and addressing these attack vectors is essential for organizations to develop effective security strategies and implement appropriate countermeasures to protect their systems, networks, and data from potential threats.

2.8.3 Cybercrime and Cloud Computing

🎬 Nowadays, prime area of the risk in cloud computing is protection of user data. Although cloud computing is an emerging field, the idea has been evolved over few years. 🎬 Risks associated with cloud computing environment are as follows

1. Elevated user access-Any data processed outside the organization brings with it an inherent level of risk
2. Regulatory compliance-Cloud computing service providers are not able and/or not willing to undergo external assessments.
3. Location of the data-User doesn't know where the data is stored or in which country it is hosted.
4. Segregation of data-Data of one organization is scattered in different locations
5. Recovery of the data-In case of any disaster, availability of the services and data is critical.
6. Information security- violation reports Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity
7. Long-term viability- In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.

Cyber Offenses