UNIT-I

Chapter 1: Introduction to Cyber Space

History of Internet and World Wide Web (WWW)

The Internet is a global system of interconnected computer networks that use the standardized Internet Protocol Suite (TCP/IP). It is a network of networks that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies. The Internet carries a vast array of information resources and services, most notably the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail, in addition to popular services such as online chat, file transfer and file sharing, online gaming, and Voice over Internet Protocol (VoIP) person-to-person communication via voice and video. The origins of the Internet dates back to the 1960s when the United States funded research projects of its military agencies to build robust, fault-tolerant and distributed computer networks. This research and a period of civilian funding of a new U.S. backbone by the National Science Foundation spawned worldwide participation in the development of new networking technologies and led to the commercialization of an international network in the mid-1990s, and resulted in the following popularization of countless applications in virtually every aspect of modern human life.

The terms Internet and World Wide Web are often used in everyday speech without much distinction. However, the Internet and the World Wide Web are not one and the same. The Internet is a global data communications system. It is a hardware and software infrastructure that provides connectivity between computers. In contrast, the Web is one of the services communicated via the Internet. It is a collection of interconnected documents and other resources, linked by hyperlinks and Uniform Resource Locator [URLs].

The World Wide Web was invented in 1989 by the English physicist Tim Berners-Lee, now the Director of the World Wide Web Consortium, and later assisted by Robert Cailliau, a Belgian computer scientist, while both were working at CERN in Geneva, Switzerland. In 1990, they proposed building a "web of nodes" storing "hypertext pages" viewed by

"browsers" on a network and released that web in December.

What is the Internet ?

Internet is an electronic communications network that connects computer networks and organizational computer facilities around the world. The internet is a globally connected network system facilitating worldwide communication and access to data resources through a vast collection of private, public, business, academic and government networks.

Evolution of Internet

The Internet was the result of some visionary thinking by people in the early 1960s who saw great potential value in allowing computers to share information on research and development in scientific and military fields. J.C.R. Licklider of MIT first proposed a global network of computers in 1962 and moved over to the Defense Advanced Research Projects Agency (DARPA) in late 1962 to head the work to develop it. Leonard Kleinrock of MIT and later UCLA developed the theory of packet switching, which was to form the basis of Internet connections. Lawrence Roberts of MIT connected a Massachusetts computer with a California computer in 1965 over dial-up telephone lines. It showed the feasibility of wide area networking, but also showed that the telephone line's circuit switching was inadequate. Kleinrock's packet switching theory was confirmed. Roberts moved over to DARPA in 1966 and developed his plan for ARPANET. These visionaries and many more left unnamed here are the real founders of the Internet.

The Internet, then known as ARPANET, was brought online in 1969 under a contract let by the renamed Advanced Research Projects Agency (ARPA) which initially connected four major computers at universities in the southwestern US (UCLA, Stanford Research Institute, UCSB, and the University of Utah). The contract was carried out by BBN of Cambridge, MA under Bob Kahn and went online in December 1969. By June 1970, MIT, Harvard, BBN, and Systems Development Corp (SDC) in Santa Monica, Cal. were added. By January 1971, Stanford, MIT's Lincoln Labs, Carnegie-Mellon, and Case-Western Reserve U were added. In months to come, NASA/Ames, Mitre, Burroughs, RAND, and the U of Illinois plugged in. After that, there were far too many to keep listing here. The Internet was designed to provide a

communications network that would work even if some of the major sites were down. If the most direct route was not available, routers would direct traffic around the network via alternate routes. The early Internet was used by computer experts, engineers, scientists, and librarians. There was nothing friendly about it. There were no home or office personal computers in those days, and anyone who used it, whether a computer professional or an engineer or scientist or librarian, had to learn to use a very complex system.

E-mail was adapted for ARPANET by Ray Tomlinson of BBN in 1972. He picked the @ symbol from the available symbols on his teletype to link the username and address. The telnet protocol, enabling logging on to a remote computer, was published as a Request for Comments (RFC) in 1972. RFC's are a means of sharing developmental work throughout community. The ftp protocol, enabling file transfers between Internet sites, was published as an RFC in 1973, and from then on RFC's were available electronically to anyone who had use of the ftp protocol.

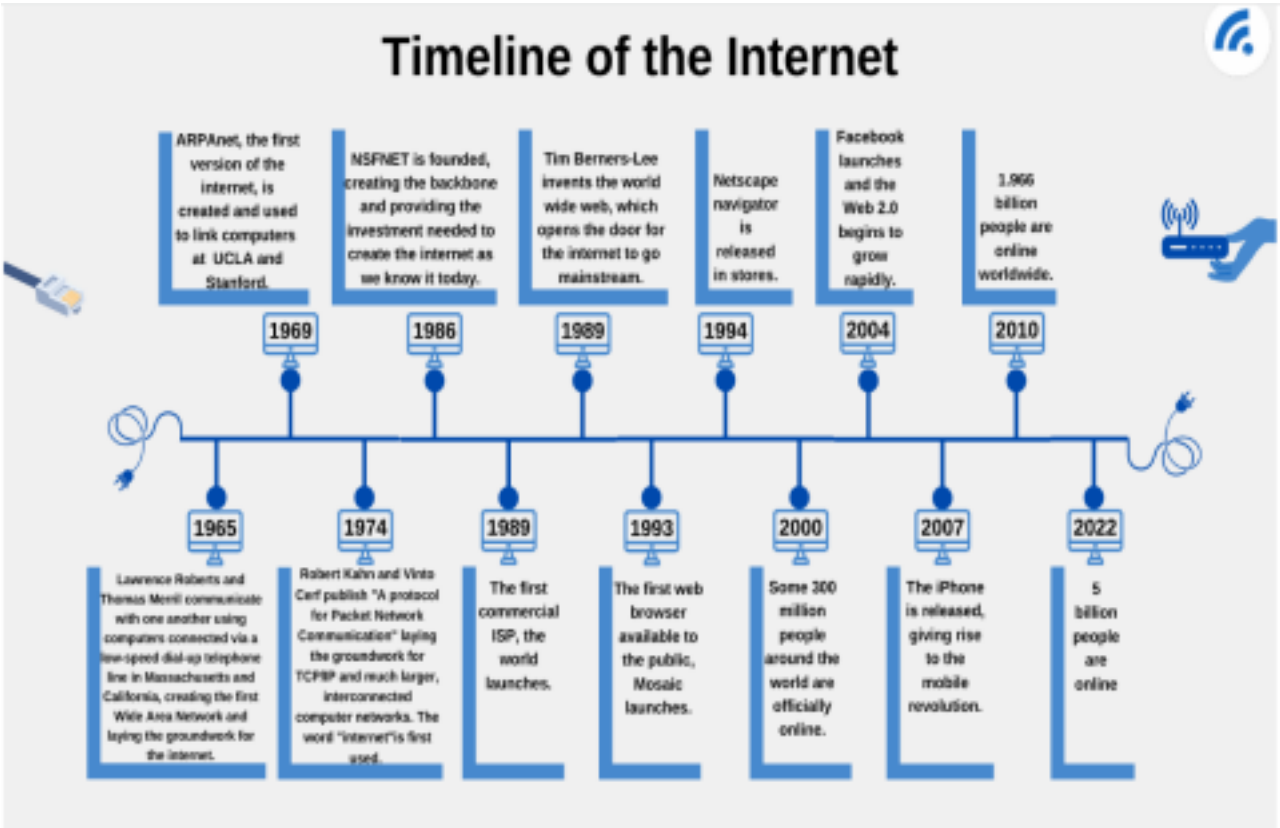


Fig 1.1 Timeline and Evaluation of internet

Applications of internet

We can roughly separate internet applications into the following types: online media, online information search, online communications, online communities, online entertainment, e business, online finance, and other applications. The internet is treated as one of the biggest invention. It has a large number of uses.

1. Communication
2. Job searches
3. Finding books and study material
4. Health and medicine
5. Travel
6. Entertainment
7. Shopping
8. Stock market updates
9. Research
10. Business use of internet: different ways by which internet can be used for business are:

I. Information about the product can be provided can be provided online to the the customer .
II. Provide market information to the business
III. It help business to recruit talented people
IV. Help in locating suppliers of the product
V. Fast information regarding customers view about companies product VI. Eliminate middle men and have a direct contact with contact with customer VII. Providing information to the investor by providing companies background and financial information on website.

How Internet Works?

The Internet is a network of networks—millions of them, actually. If the network at your university, your employer, or in your home has Internet access, it connects to an Internet service provider (ISP). Many (but not all) ISPs are big telecommunications companies like Verizon, Comcast, and AT&T. These providers connect to one another, exchanging traffic, and ensuring

your messages can get to any other computer that's online and willing to communicate with you.

The Internet has no center and no one owns it. That's a good thing. The Internet was designed to be redundant and fault-tolerant—meaning that if one network, connecting wire, or server stops working, everything else should keep on running. Rising from military research and work at educational institutions dating as far back as the 1960s, the Internet really took off in the 1990s, when graphical Web browsing was invented, and much of the Internet's operating infrastructure was transitioned to be supported by private firms rather than government grants.

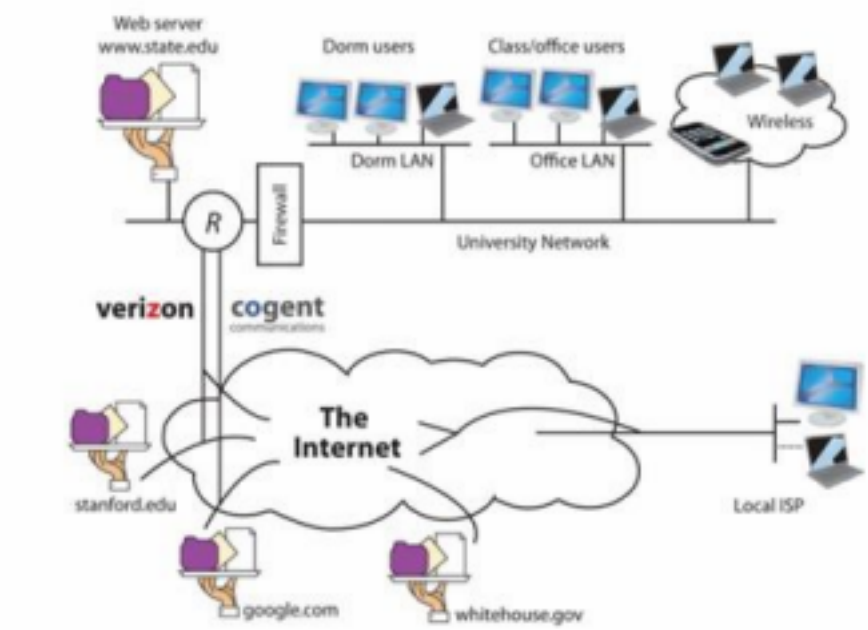


Fig 1.2 Working of the Internet

Enough history—let's see how it all works! If you want to communicate with another computer on the Internet then your computer needs to know the answer to three questions: What are you looking for? Where is it? And how do we get there? The computers and software that make up Internet infrastructure can help provide the answers. Let's look at how it all comes together.

When you type an address into a Web browser (sometimes called a URL for uniform resource locator), you're telling your browser what you're looking for, Figure 2 describes how to read a typical URL.

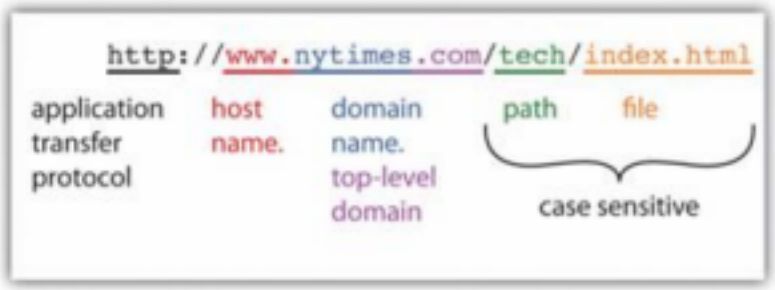


Fig 1.3 Anatomy of a Web Address

The http:// you see at the start of most Web addresses stands for hypertext transfer protocol. A protocol is a set of rules for communication—sort of like grammar and vocabulary in a language like English. The http protocol defines how Web browser and Web servers communicate and is designed to be independent from the computer's hardware and operating system. It doesn't matter if messages come from a PC, a Mac, a huge mainframe, or a pocket sized smartphone; if a device speaks to another using a common protocol, then it will be heard and understood. The Internet supports lots of different applications, and many of these applications use their own application transfer protocol to communicate with each other. The server that holds your e-mail uses something called SMTP, or simple mail transfer protocol, to exchange mail with other e-mail servers throughout the world. FTP, or file transfer protocol, is used for—you guessed it—file transfer. FTP is how most Web developers upload the Web pages, graphics, and other files for their Web sites. Even the Web uses different protocols. When you surf to an online bank or when you're ready to enter your payment information at the Web site of an Internet retailer, the http at the beginning of your URL will probably change to https (the "s" is for secure). That means that communications between your browser and server will be encrypted for safe transmission. The beauty of the Internet infrastructure is that any savvy entrepreneur can create a new application that rides on top of the Internet.

Introduction to cyber space

Cyberspace- Definition

"Cyberspace refers to the **virtual space** that provides the **infrastructure, electronic medium** and **related elements** necessary for online global communication"

Fig.1.4 Cyberspace

Why Cyber Security is important?

- Cyber Security is not a one-time process to achieve
- It is an ever-growing challenge encountered from time to time
- When old problems are fixed and rectified, new targeted attacks challenge the Cyberspace
- Cyber security is a process by itself and not the end

Hackers

- Hackers are unauthorized users of a system.
- They invade a system through the vulnerabilities or weak points in the system. • They make use of large diverse tools to harm a computer system.
- They gain access to computer systems through malicious logic.

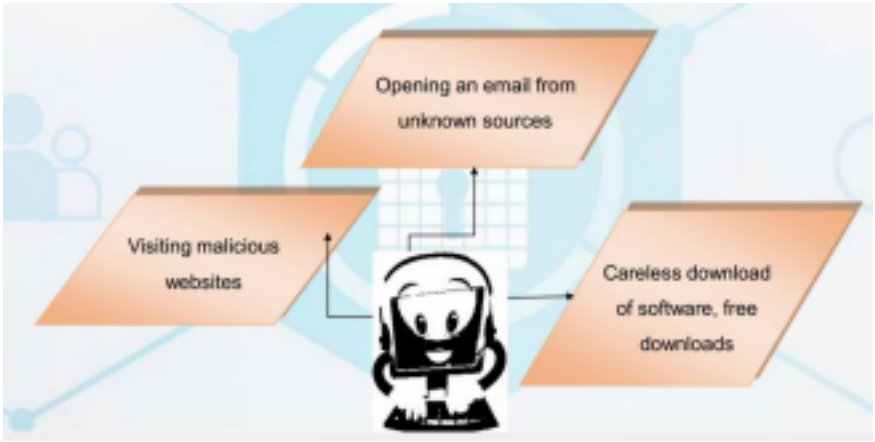


Fig 1.5. Common ways a computer can become infected

History and evolution of Information Security and cyber-Security

What is the origin of information security?

In the 1970s, the true birth of cybersecurity began with a project called The Advanced Research Projects Agency Network (ARPANET). ARPANET was the network developed prior to the internet.

Fig 1.6. Information security

Principle of Information System Security : History

Information security (IS) is designed to protect the confidentiality, integrity and availability of data from those with malicious intentions of misusing that data in many manners. These are set of techniques used for managing the tools and policies to prevent and detect information stored in digital or non-digital media. It is often confused with Cyber security but Information Security (IS) is a crucial part of Cyber security, but it refers exclusively to the processes designed for data security. Cyber security is a more general term that includes Information Security as crucial part of itself. **History of Information Security:** These days, information plays an important role in day to day lives of every individual, whether it be a

high profile businessman to being a small shop owner. Information is generated in different forms from being their smartphones to their transaction receipts and buying patterns. This presents a wealth of opportunities for people to steal data; that is why information security is a necessity. But how has information security evolved over the years? Let's take a look at the history of information security and how it evolved on the course of this duration. **1960s: Offline sites security:** The Information Security was limited to the access points where computers were stored, as they used to be large in sizes and required a huge area to be stored and operated. Multiple layers of security were installed over terminals in form of passwords and other security measures. **1970s: Evolution of personal computer and hackers:** At this time there was no massive global network connecting every device that wanted to be connected. Only large organizations, especially governments, were starting to link computers via telephone lines and peoples started to seek different ways to intercept the information flowing through those telephone lines in order to steal the data and these group of peoples became the first hackers. **1980s: Evolution of cyber-crime:** Hacking and other forms of cyber crimes skyrocketed in this decade with people finding different ways to break into the computer systems and being no strict regulation against the hackers it was a booming craze for the youth. Many government & Military groups were on the receiving end of these crimes with loss of over millions of dollars from U.S. Banks and in response to this the government started pursuing the hackers. **1990s: "Hacking" becoming an organized crime:** After the worldwide web was made available in 1989, people started putting their personal information online; hackers saw this as a potential revenue source, and started to steal data from people and governments via the web. Firewalls and antivirus programs helped protect against this, but the web was a mostly unsecured with hackers finding different ways to infiltrate the targets devices. **2000s: Cybercrime becoming a serious issue:** Hacking wasn't considered as serious issues in late 80's but with evolution of hacking and their dangers governments started chasing the cyber criminals. Strong measures were taken against cyber criminals, hackers were jailed for years as punishment for cyber criminal activity and cyber security cells were formed to deal with the issues involving any form of cyber crime. **2010s: Information security as we know it:** Although different measures in form of firewalls and antivirus were designed to protect the devices from attacks but hackers who were efficient

and skilled enough were able to breach the systems anyway. Different cryptographic algorithms and encryption techniques are being used in order to protect the data over network and other transmission mediums. Different organizations also implement security policies to avoid human errors of breaching the data in different ways. Software and antivirus programs are installed on PC's to protect them from the outside attacks. With time as the internet and devices surrounding the internet evolved, the threat to the information security also found many ways to breach into them. Information security plays a major role in day-to-day life of every person and organizations.

Principle of Information System Security : Security System Development Life Cycle

Security System Development Life Cycle (SecSDLC) is defined as the set of procedures that are executed in a sequence in the software development cycle (SDLC). It is designed such that it can help developers to create software and applications in a way that reduces the security risks at later stages significantly from the start. The Security System Development Life Cycle (SecSDLC) is similar to Software Development Life Cycle (SDLC), but they differ in terms of the activities that are carried out in each phase of the cycle. SecSDLC eliminates security vulnerabilities. Its process involves identification of certain threats and the risks they impose on a system as well as the needed implementation of security controls to counter, remove and manage the risks involved. Whereas, in the SDLC process, the focus is mainly on the designs and implementations of an information system. **Phases involved in SecSDLC are:**

System Investigation: This process is started by the officials/directives working at the top level management in the organization. The objectives and goals of the project are considered priorly to execute this process. An Information Security Policy is defined which contains the descriptions of security applications and programs installed along with their implementations in organization's system.

System Analysis: In this phase, detailed document analysis of the documents from the System Investigation phase are done. Already existing security policies, applications and software are analyzed to check for different flaws and vulnerabilities in the system.

Upcoming threat possibilities are also analyzed. Risk management comes under this process only.

Logical Design: The Logical Design phase deals with the development of tools and following blueprints that are involved in various information security policies, their applications and software. Backup and recovery policies are also drafted in order to prevent future losses. In case of any disaster, the steps to take in business are also planned. The decision to outsource the company project is decided in this phase. It is analyzed whether the project can be completed in the company itself or it needs to be sent to another company for the specific task.

Physical Design: The technical teams acquire the tools and blueprints needed for the implementation of the software and application of the system security. During this phase, different solutions are investigated for any unforeseen issues which may be encountered in the future. They are analyzed and written down to cover most of the vulnerabilities that were missed during the analysis phase.

Implementation: The solution decided in earlier phases is made final whether the project is in-house or outsourced. The proper documentation is provided of the product to meet the requirements specified for the project to be met. Implementation and integration process of the project are carried out with the help of various teams aggressively testing whether the product meets the system requirements specified in the system documentation.

Maintenance: After the implementation of the security program, it must be ensured that it is functioning properly and is managed accordingly. The security program must be kept up to date accordingly to counter new threats that can be left unseen at the time of design.

Difference between Cyber Security and Information Security

The terms Cyber Security and Information Security are often used interchangeably. As they both are responsible for the security and protecting the computer system from threats and information breaches and often Cybersecurity and information security are so closely linked that they may seem synonymous and unfortunately, they are used synonymously. If we talk about data security, it’s all about securing the data from malicious users and threats. Now another question is what is the difference between Data and Information? So one important point is that “not every data can be information” data can be informed if it is interpreted in a

context and given meaning. for example, “100798” is data and if we know that it’s the date of birth of a person then it is information because it has some meaning. so information means data that has some meaning. Examples and Inclusion of Cyber Security are as follows: • Network Security

- Application Security
- Cloud Security
- Critical Infrastructure

Examples and inclusion of Information Security are as follows:

- Procedural Controls
- Access Controls
- Technical Controls
- Compliance Controls

Parameters	CYBER SECURITY	INFORMATION SECURITY
Basic Definition	It is the practice of protecting the data from outside the resource on the internet.	It is all about protecting information from unauthorized users, access, and data modification or removal in order to provide confidentiality, integrity, and availability.
Protect	It is about the ability to protect the use of cyberspace from cyber attacks.	It deals with the protection of data from any form of threat.
Scope	Cybersecurity to protect anything in the cyber realm.	Information security is for information irrespective of the realm.
Threat	Cybersecurity deals with the danger in cyberspace.	Information security deals with the protection of data from any form of threat.
Attacks	Cybersecurity strikes against Cyber crimes, cyber frauds, and law enforcement.	Information security strikes against unauthorized access, disclosure modification, and disruption.
Professionals	Cyber security professionals deal with the prevention of active threats or Advanced Persistent threats (APT).	Information security professionals are the foundation of data security and security professionals associated with it are responsible for policies, processes, and organizational roles and responsibilities that assure confidentiality, integrity, and availability.
Deals with	It deals with threats that may or may not exist in the cyber realm such as protecting your social media account, personal information, etc.	It deals with information Assets and integrity, confidentiality, and availability.
Defense	Acts as first line of defense.	Comes into play when security is breached.

Difference between Information Security and Network Security

Information Security is the measures taken to protect the information from unauthorized access and use. It provides confidentiality, integrity, and availability. It is the superset that contains cyber security and network security. It is necessary for any organization or firm that works on a large scale. Examples and inclusion of Information Security are as follows:

- Procedural Controls
- Access Controls
- Technical Controls
- Compliance Controls

Network Security: Network Security is the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats. Examples and inclusion of Network Security are as follows:

- Firewall
- Network Segmentation
- Remote Access VPN
- Email Security
- Intrusion Prevention Systems (IPS)
- Sandboxing
- Hyperscale Network Security.
- Data Loss Prevention (DLP)

Parameters	Information Security	Network Security
Data	It protects information from unauthorized users, access, and data modification.	It protects the data flowing over the network.
Part of	It is a superset of cyber security and network security.	It is a subset of cyber security.
Protection	Information security is for information irrespective of the realm.	It protects anything in the network realm.
Attack	It deals with the protection of data from any form of threat.	It deals with the protection from DOS attacks.
Scope	It strikes against unauthorized access, disclosure modification, and disruption.	Network Security strikes against trojans.
Usage	It provides confidentiality, integrity, and availability.	It provides security over the network only.
Ensures	Information security ensures to the protection of transit and stationary data.	Network security ensures to protect the transit data only.
Deals with	It deals with information assets and integrity, confidentiality, and availability.	It secures the data traveling across the network by terminals.

What is Cyber Security?

The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**.

Definitions of cybersecurity

- Cybersecurity is the practice of protecting critical systems and sensitive information from **digital attacks.**
- **Cyber security** is the practice of **defending computers, servers, mobile devices, electronic systems, networks**, and **data from malicious attacks**.
- *"Cyber Security is the **body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access**."*
- *"Cyber Security is the **set of principles and practices designed to protect our computing resources and online information against threats**."*

Types of Cyber Security

Every organization's assets are the combinations of a variety of different systems. These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cybersecurity in the following sub-domains:

- **Network Security:** It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
- **Application Security:** It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.
- **Information or Data Security:** It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security:** It involves processing and making decisions on handling and securing data assets.
- **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.

- **Cloud Security:** It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.
- **Disaster Recovery and Business Continuity Planning:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.
- **User Education:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

Why is Cyber Security important?

Today we live in a digital era where all aspects of our lives depend on the network, computer and other electronic devices, and software applications. All critical infrastructure such as the banking system, healthcare, financial institutions, governments, and manufacturing industries use **devices connected to the Internet** as a core part of their operations. Some of their information, such as intellectual property, financial data, and personal data, can be sensitive for unauthorized access or exposure that could have **negative consequences**. This information gives intruders and threat actors to infiltrate them for financial gain, extortion, political or social motives, or just vandalism.

Cyber-attack is now an international concern that hacks the system, and other security attacks could endanger the global economy. Therefore, it is essential to have an excellent cybersecurity strategy to protect sensitive information from high-profile security breaches. Furthermore, as the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to use strong cybersecurity measures and processes to protect their sensitive business and personal information.

Cyber Security Goals

main objective is to ensure data protection. The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the CIA triad. The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated. We can break the CIA model into three parts: Confidentiality, Integrity, and Availability. It is a security model that helps people to think about various parts of IT security. Let us discuss each part in detail.

Confidentiality: Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. **Data encryption** is an excellent example of ensuring confidentiality.

Integrity: This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.

Availability: This principle makes the information to be available and useful for its

authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber attacks.

Types of Cyber Security Threats

A threat in cybersecurity is a malicious activity by an individual or organization to corrupt or steal data, gain access to a network, or disrupts digital life in general. The cyber community defines the following threats available today:

Malware

Malware means malicious software, which is the most common cyber attacking tool. It is used by the cybercriminal or hacker to disrupt or damage a legitimate user's system. The following are the important types of malware created by the hacker:

- **Virus**: It is a malicious piece of code that spreads from one device to another. It can clean files and spreads throughout a computer system, infecting files, stoles information, or damage device.

- **Spyware**: It is a software that secretly records information about user activities on their system. **For example**, spyware could capture credit card details that can be used by

the cybercriminals for unauthorized shopping, money withdrawing, etc.

- **Trojans**: It is a type of malware or code that appears as legitimate software or file to fool us into downloading and running. Its primary purpose is to corrupt or steal data from our device or do other harmful activities on our network.
- **Ransomware**: It's a piece of software that encrypts a user's files and data on a device, rendering them unusable or erasing. Then, a monetary ransom is demanded by malicious actors for decryption.
- **Worms**: It is a piece of software that spreads copies of itself from device to device without human interaction. It does not require them to attach themselves to any program to steal or damage the data.
- **Adware**: It is an advertising software used to spread malware and displays advertisements on our device. It is an unwanted program that is installed without the user's permission. The main objective of this program is to generate revenue for its developer by showing the ads on their browser.
- **Botnets**: It is a collection of internet-connected malware-infected devices that allow cybercriminals to control them. It enables cybercriminals to get credentials leaks, unauthorized access, and data theft without the user's permission.

Phishing

Phishing is a type of cybercrime in which **a sender seems to come from a genuine organization** like PayPal, eBay, financial institutions, or friends and co-workers. They contact a target or targets via email, phone, or text message with a link to persuade them to click on that links. This link will redirect them to fraudulent websites to provide sensitive data such as personal information, banking and credit card information, social security numbers, usernames, and passwords. Clicking on the link will **also install malware** on the target devices that allow hackers to control devices remotely.

Man-in-the-middle (MITM) attack

A man-in-the-middle attack is a type of cyber threat (a form of eavesdropping attack) in which

a cybercriminal **intercepts a conversation or data transfer between two individuals**. Once the cybercriminal places themselves in the middle of a two-party communication, they seem like genuine participants and can get sensitive information and return different responses. The main objective of this type of attack is to gain access to our business or customer data. **For example**, a cybercriminal could intercept data passing between the target device and the network on an unprotected Wi-Fi network.

Distributed denial of service (DDoS)

It is a type of cyber threat or malicious attempt where cybercriminals disrupt targeted servers, services, or network's regular traffic by fulfilling legitimate requests to the target or its surrounding infrastructure with Internet traffic. Here the requests come from several IP addresses that can make the system unusable, overload their servers, slowing down significantly or temporarily taking them offline, or preventing an organization from carrying out its vital functions.

Brute Force

A brute force attack is a **cryptographic hack that uses a trial-and-error method** to guess all possible combinations until the correct information is discovered. Cybercriminals usually use this attack to obtain personal information about targeted passwords, login info, encryption keys, and Personal Identification Numbers (PINS).

SQL Injection (SQLI)

SQL injection is a common attack that occurs when cybercriminals use malicious SQL scripts for backend database manipulation to access sensitive information. Once the attack is successful, the malicious actor can view, change, or delete sensitive company data, user lists, or private customer details stored in the SQL database.

Domain Name System (DNS) attack

A DNS attack is a type of cyberattack in which cyber criminals take advantage of flaws in the

Domain Name System to redirect site users to malicious websites (DNS hijacking) and steal data from affected computers. It is a severe cybersecurity risk because the DNS system is an essential element of the internet infrastructure.

Latest cyber threats

The following are the latest cyber threats reported by the U.K., U.S., and Australian governments:

Romance Scams

The U.S. government found this cyber threat in **February 2020**. Cybercriminals used this threat through dating sites, chat rooms, and apps. They attack people who are seeking a new partner and duping them into giving away personal data.

Dridex Malware

It is a type of financial Trojan malware identifies by the U.S. in **December 2019** that affects the public, government, infrastructure, and business worldwide. It infects computers through phishing emails or existing malware to steal sensitive information such as passwords, banking details, and personal data for fraudulent transactions. The National Cyber Security Centre of the United Kingdom encourages people to make sure their devices are patched, anti-virus is turned on and up to date, and files are backed up to protect sensitive data against this attack.

Emotet Malware

Emotet is a type of cyber-attack that steals sensitive data and also installs other malware on our device. The Australian Cyber Security Centre warned national organizations about this global cyber threat in 2019.

The following are the system that can be affected by security breaches and attacks:

- **Communication**: Cyber attackers can use phone calls, emails, text messages, and messaging apps for cyberattacks.
- **Finance**: This system deals with the risk of financial information like bank and credit

card detail. This information is naturally a primary target for cyber attackers. • **Governments**: The cybercriminal generally targets the government institutions to get confidential public data or private citizen information.

- **Transportation**: In this system, cybercriminals generally target connected cars, traffic control systems, and smart road infrastructure.
- **Healthcare**: A cybercriminal targets the healthcare system to get the information stored at a local clinic to critical care systems at a national hospital.
- **Education**: A cybercriminals target educational institutions to get their confidential research data and information of students and employees**.**

Benefits of cybersecurity

The following are the benefits of implementing and maintaining cybersecurity:

- Cyberattacks and data breach protection for businesses.
- Data and network security are both protected.
- Unauthorized user access is avoided.
- After a breach, there is a faster recovery time.
- End-user and endpoint device protection.
- Regulatory adherence.
- Continuity of operations.
- Developers, partners, consumers, stakeholders, and workers have more faith in the company's reputation and trust.

Cyber Safety Tips

Let us see how to protect ourselves when any cyberattacks happen. The following are the popular cyber safety tips:

Conduct cybersecurity training and awareness: Every organization must train their staffs on cybersecurity, company policies, and incident reporting for a strong cybersecurity policy to be successful. If the staff does unintentional or intentional malicious activities, it may fail the

best technical safeguards that result in an expensive security breach. Therefore, it is useful to conduct security training and awareness for staff through seminars, classes, and online courses that reduce security violations.

Update software and operating system: The most popular safety measure is to update the software and O.S. to get the benefit of the latest security patches.

Use anti-virus software: It is also useful to use the anti-virus software that will detect and removes unwanted threats from your device. This software is always updated to get the best level of protection.

Perform periodic security reviews: Every organization ensures periodic security inspections of all software and networks to identify security risks early in a secure environment. Some popular examples of security reviews are application and network penetration testing, source code reviews, architecture design reviews, and red team assessments. In addition, organizations should prioritize and mitigate security vulnerabilities as quickly as possible after they are discovered.

Use strong passwords: It is recommended to always use long and various combinations of characters and symbols in the password. It makes the passwords are not easily guessable.

Do not open email attachments from unknown senders: The cyber expert always advises not to open or click the email attachment getting from unverified senders or unfamiliar websites because it could be infected with malware.

Avoid using unsecured Wi-Fi networks in public places: It should also be advised not to use insecure networks because they can leave you vulnerable to man-in-the-middle attacks.

Backup data: Every organization must periodically take backup of their data to ensure all sensitive data is not lost or recovered after a security breach. In addition, backups can help maintain data integrity in cyber-attack such as SQL injections, phishing, and ransomware.

Computer ethics

Ten Commandments of Computer Ethics

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid (without permission).
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for other humans.

Commandment 1: Thou shalt not use a computer to harm other people.

Simply put: Do not use the computer in ways that may harm other people. Explanation: This commandment says that it is unethical to use a computer to harm another user. It is not limited to physical injury. It includes harming or corrupting other users' data or files. The commandment states that it is wrong to use a computer to steal someone's personal information. Manipulating or destroying files of other users is ethically wrong. It is unethical to write programs, which on execution lead to stealing, copying or gaining unauthorized access to other users' data. Being involved in practices like hacking, spamming, phishing or cyber bullying does not conform to computer ethics.

Commandment 2: Thou shalt not interfere with other people's computer work.

Simply put: Do not use computer technology to cause interference in other users' work. Explanation: Computer software can be used in ways that disturb other users or disrupt their work. Viruses, for example, are programs meant to harm useful computer programs or

interfere with the normal functioning of a computer. Malicious software can disrupt the functioning of computers in more ways than one. It may overload computer memory through excessive consumption of computer resources, thus slowing its functioning. It may cause a computer to function wrongly or even stop working. Using malicious software to attack a computer is unethical.

Commandment 3: Thou shalt not snoop around in other people's computer files.

Simply put: Do not spy on another person's computer data.

Explanation: We know it is wrong to read someone's personal letters. On the same lines, it is wrong to read someone else's email messages or files. Obtaining data from another person's private files is nothing less than breaking into someone's room. Snooping around in another person's files or reading someone else's personal messages is the invasion of his privacy. There are exceptions to this. For example, spying is necessary and cannot be called unethical when it is done against illegitimate use of computers. For example, intelligence agencies working on cybercrime cases need to spy on the internet activity of suspects.

Commandment 4: Thou shalt not use a computer to steal.

Simply put: Do not use computer technology to steal information.

Explanation: Stealing sensitive information or leaking confidential information is as good as robbery. It is wrong to acquire personal information of employees from an employee database or patient history from a hospital database or other such information that is meant to be confidential. Similarly, breaking into a bank account to collect information about the account or account holder is wrong. Illegal electronic transfer of funds is a type of fraud. With the use of technology, stealing of information is much easier. Computers can be used to store stolen information.

Commandment 5: Thou shalt not use a computer to bear false witness.

Simply put: Do not contribute to the spread of misinformation using computer technology.

Explanation: Spread of information has become viral today, because of the Internet. This also means that false news or rumors can spread speedily through social networking sites or emails. Being involved in the circulation of incorrect information is unethical. Mails and pop-ups are commonly used to spread the wrong information or give false alerts with the only

intent of selling products. Mails from untrusted sources advertising certain products or spreading some hard-to-believe information, are not uncommon. Direct or indirect involvement in the circulation of false information is ethically wrong. Giving wrong information can hurt other parties or organizations that are affected by that particular theme.

Commandment 6: Thou shalt not copy or use proprietary software for which you have not paid (without permission).

Simply put: Refrain from copying software or buying pirated copies. Pay for software unless it is free.

Explanation: Like any other artistic or literary work, software is copyrighted. A piece of code is the original work of the individual who created it. It is copyrighted in his/her name. In case of a developer writing software for the organization she works for, the organization holds the copyright for it. Copyright holds true unless its creators announce it is not. Obtaining illegal copies of copyrighted software is unethical and also encourages others to make copies illegally.

Commandment 7: Thou shalt not use other people's computer resources without authorization or proper compensation.

Simply put: Do not use someone else's computer resources unless authorized to. Explanation: Multi-user systems have user specific passwords. Breaking into some other user's password, thus intruding his/her private space is unethical. It is not ethical to hack passwords for gaining unauthorized access to a password-protected computer system. Accessing data that you are not authorized to access or gaining access to another user's computer without her permission is not ethical.

Commandment 8: Thou shalt not appropriate other people's intellectual output.

Simply put: It is wrong to claim ownership on a work which is the output of someone else's intellect.

Explanation: Programs developed by a software developer are her property. If he is working with an organization, they are the organization's property. Copying them and propagating them in one's own name is unethical. This applies to any creative work, program or design.

Establishing ownership on a work which is not yours is ethically wrong.

Commandment 9: Thou shalt think about the social consequences of the program you are writing or the system you are designing.

Simply put: Before developing a software, think about the social impact it can have.
Explanation: Looking at the social consequences that a program can have, describes a broader perspective of looking at technology. A computer software on release, reaches millions. Software like video games and animations or educational software can have a social impact on their users. When working on animation films or designing video games, for example, it is the programmer's responsibility to understand his target audience/users and the effect it may have on them. For example, a computer game for kids should not have content that can influence them negatively. Similarly, writing malicious software is ethically wrong. A software developer/development firm should consider the influence their code can have on the society at large.

Commandment 10: Thou shalt always use a computer in ways that ensure consideration and respect for other humans.

Simply put: In using computers for communication, be respectful and courteous with the fellow members.

Explanation: The communication etiquette we follow in the real world applies to communication over computers as well. While communicating over the Internet, one should treat others with respect. One should not intrude others' private space, use abusive language, make false statements, or pass irresponsible remarks about others. One should be courteous while communicating over the web and should respect others' time and resources. Also, one should be considerate with a novice computer user.

Cyber Security Policy

Cyberspace is a complex environment consisting of interactions between people, software, and services, supported by the worldwide distribution of information and communication technology (ICT) devices and networks.

Cybersecurity plays a crucial role within the field of the digital world. Securing information

and data became one of the most important challenges within the present day. Whenever we expect cybersecurity the primary thing that involves our mind is cybercrimes which are increasing immensely day by day. Various Governments and Organizations are taking many measures to stop these cybercrimes. Besides various measures, cybersecurity remains a massive concern to several. The top three cybersecurity trends in 2021 are:

- Ransomware
- Cyber-attack Surface (IoT supply chain and Remote work systems)
- Threats to IT infrastructure

In the extensive growth of the IT sector in the different country, ambitious plans for rapid social transformation and inclusive growth, and providing the right kind of focus for creating a secure computing environment and adequate trust and confidence in electronic transactions, software, services, devices, and networks, has become one of the compelling priorities for all.

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in cyberspace can be exploited for nefarious purposes. The protection of information cyberspace and preservation of the confidentiality, integrity, and availability of information in cyberspace is the essence of secure cyberspace.

Acceptable Use of data Systems Policy-The purpose of this policy is to stipulate the suitable use of computer devices at the corporate/company. These rules protect the authorized user and therefore the company also. Inappropriate use exposes the corporate to risks including virus attacks, compromise of network systems and services, and legal issues.

Account Management Policy-The purpose of this policy is to determine a typical for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at the corporate.

Anti-Virus- This policy was established to assist prevent attacks on corporate computers, networks, and technology systems from malware and other malicious code. This policy is meant to assist prevent damage to user applications, data, files, and hardware. Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it

can check for the new viruses as soon as they are discovered. Anti-virus software is a must and a necessity for every system.

E-Commerce Policy- The frequency of cyber-attacks has high in recent years. Ecommerce security refers to the measures taken to secure businesses and their customers against cyber threats. This e-commerce policy is to be used as both a suggestion and a summary within the management of the E-Commerce electronic services.

E-Mail Policy- Email security may be a term for describing different procedures and techniques for shielding email accounts, content, and communication against unauthorized access, loss, or compromise. Email is usually wont to spread malware, spam, and phishing attacks. Attackers use deceptive messages to entice recipients to spare sensitive information, open attachments, or click on hyperlinks that install malware on the victim's device. Email is additionally a standard entry point for attackers looking to realize an edge in an enterprise network and acquire valuable company data. Email encryption involves encrypting, or disguising, the content of email messages to guard potentially sensitive information against being read by anyone aside from intended recipients. Email encryption often includes authentication. The purpose of this policy is to determine rules for the utilization of corporate email for sending, receiving, or storing electronic messages.

Hardware And Electronic Media Disposal Policy-The company-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this policy. This policy will esablish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner.

Security Incident Management Policy- This policy defines the need for reporting and

responding to incidents associated with the company's information systems and operations. Incident response provides the corporate with the potential to spot when a security incident occurs.

Information Technology Purchasing Policy-The reason for this strategy is to characterize norms, methods, and limitations for the acquisition of all IT equipment, programming, PC related parts, and specialized administrations bought with organization reserves. Acquisition of innovation and specialized administrations for the organization should be supported and facilitated through the IT Department.

Web Policy-The reason for this policy is to set up the guidelines for the utilization of the organization's Internet for access to the Internet or the Intranet.

Log Management Policy - Log management is often of great benefit during a sort of scenario, with proper management, to reinforce security, system performance, resource management, and regulatory compliance.

Network Security and VPN Acceptable Use Policy- The purpose of this policy is to define standards for connecting to the company's network from any host. These standards are designed to attenuate the potential exposure to the corporate from damages, which can result from unauthorized use of the company's resources. Damages include the loss of sensitive or company confidential data, property, damage to critical company internal systems, etc.

Password Policy- The concept of username and passwords has been a fundamental way of protecting our information. This may be one of the first measures regarding cybersecurity. The purpose of this policy is to determine a typical for the creation of strong passwords, the protection of these passwords, and therefore the frequency of change password must be followed.

Patch Management Policy-Security vulnerabilities are inherent in computing systems and applications. These flaws allow the event and propagation of malicious software, which may disrupt normal business operations, additionally placing the corporate in danger. To effectively mitigate this risk, software "patches" are made available to get rid of a given security vulnerability.

Cloud Computing Adoption- The purpose of this policy is to make sure that the corporate

can potentially make appropriate cloud adoption decisions and at an equivalent time doesn't use, or allow the utilization of, inappropriate cloud service practices. Acceptable and unacceptable cloud adoption examples are listed during this policy.

Server Security Policy-The purpose of this policy is to define standards and restrictions for the bottom configuration of internal server equipment owned and/or operated by or on the company's internal network(s) or related technology resources via any channel. **Social Media Acceptable Use Policy-**The use of external social media within organizations for business purposes is increasing. The corporate faces exposure of a particular amount of data that will be visible to friends of friends from social media. While this exposure may be a key mechanism driving value, it also can create an inappropriate conduit for information to pass between personal and business contacts. Tools to determine barriers between personal and personal networks and tools to centrally manage accounts are only starting to emerge. Involvement by the IT Department for security, privacy, and bandwidth concerns is of maximal importance.

Systems Monitoring And Auditing Policy-System monitoring and auditing are employed to work out if inappropriate actions have occurred within a data system. System monitoring is employed to seem for these actions in real-time while system auditing looks for them after the very fact.

Vulnerability Assessment- The purpose of this policy is to determine standards for periodic vulnerability assessments. This policy reflects the company's commitment to spot and implement security controls, which can keep risks to data system resources at reasonable and appropriate levels.

Website Operation Policy - The purpose of this policy is to determine guidelines with reference to communication and updates of the company's public-facing website. Protecting the knowledge on and within the corporate website, with equivalent safety and confidentiality standards utilized within the transaction of all the corporate business, is significant to the company's success.

Workstation Configuration Security Policy-The purpose of this policy is to reinforce security and quality operating status for workstations utilized at the corporate. IT resources

are to utilize these guidelines when deploying all new workstation equipment. Workstation users are expected to take care of these guidelines and to figure collaboratively with IT resources to take care of the rules that are deployed.

Server Virtualization-The purpose of this policy is to determine server virtualization requirements that outline the acquisition, use, and management of server virtualization technologies. This policy provides controls that make sure that Enterprise issues are considered, alongside business objectives, when making server virtualization-related decisions. Platform Architecture policies, standards, and guidelines are going to be wont to acquire, design, implement and manage all server virtualization technologies.

Wireless Connectivity Policy-The purpose of this policy is to secure and protect the knowledge assets owned by the corporate and to determine awareness and safe practices for connecting to free and unsecured Wi-Fi, which can be provided by the corporate. The corporate provides computer devices, networks, and other electronic information systems to goals, and initiatives. The corporate grants access to those resources as a privilege and must manage them responsibly to take care of the confidentiality, integrity, and availability of all information assets.

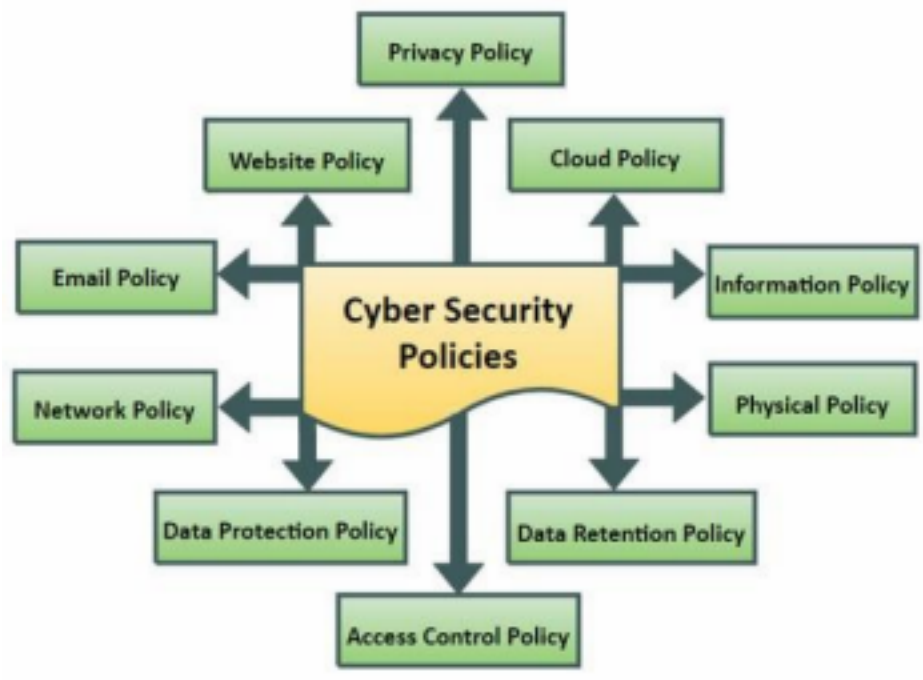
Telecommuting Policy- For the needs of this policy, reference is formed to the defined telecommuting employee who regularly performs their work from an office that's not within a corporate building or suite. Casual telework by employees or remote work by non employees isn't included herein. That specializes in the IT equipment typically provided to a telecommuter, this policy addresses the telecommuting work arrangement and therefore the responsibility for the equipment provided by the corporate.

Firewall- A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the Internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence, firewalls play an important role in detecting malware.

Malware scanner-This is software that sometimes scans all the files and documents present within the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are samples of malicious software that are often grouped together and mentioned as malware.


INFORMATION SECURITY POLICY INCLUSIONS
Access control
Identification and Authentication
Data classification
Encryption
Remote access
Acceptable use
Patching
Malicious code protections
Physical security
Backups
Server security
Employee on/offboarding
Change management
LINFORDCO.COM


Cyber Security Policies
Intrusion Prevention Policy
LiveUpdate Policy
Application and Device Control
Exceptions Policy
Host Integrity Policy
Access Control Policy
Change Management Policy
Information Security Policy


Privacy Policy
Website Policy
Cloud Policy
Email Policy
Cyber Security Policies
Information Policy
Network Policy
Physical Policy
Data Protection Policy
Data Retention Policy
Access Control Policy

Chapter 2 Introduction to Cybercrime

"Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age. Taken from *kybernetes*, Greek word for "steersman" or "governor," it was first used in cybernetics, a word coined by Norbert Wiener and his colleagues. The virtual world of internet is known as cyberspace and the laws governing this area are known as Cyber laws and allthe netizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet. The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. All these regulatory mechanisms and legal infrastructures come within the domain of Cyber law.

Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives.

Cyber law encompasses laws relating to –

- Cyber crimes
- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

Definition of Cyber Crime

- Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the

data processed by them.

- Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

• Computer-related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data. **Rise of Cyber crimes**

As per the cyber crime data maintained by the **National Crime Records Bureau (NCRB)** https://ncrb.gov.in/en According to NCRB, the police have recorded under both the Information Technology (IT) Act as well as the Indian Penal Code (IPC). 58.6% of the offenders were in the age group 18–30 years, 31.7% of the offenders were in the age group 30- 45 years and **remaining reported offenders whose age was below 18 years.**Awareness and education, labs, research centres

Important terms related to cyber law

"Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

"Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary

"Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature

"Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

"Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24

"Communication Device" means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image.

"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network

"**Computer Network"** means the interconnection of one or more Computers or Computer systems or Communication device through-

- use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
- terminals or a complex consisting of two or more interconnected computers or

communication device whether or not the interconnection is continuously maintained.

"Computer Resource" means computer, communication device, computer system, computer network, data, computer database or software.

"Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions.

"Cyber cafe" means any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public.

"Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

"Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer

network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

"Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

"Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

"**Electronic Record"** means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. **"Electronic signature"** means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature.

"Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.

"Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche.

"Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

"Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

"Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary

"Private Key" means the key of a key pair used to create a digital signature. **"Public Key"** means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate. (Sec.2(1)(zd) of IT Act, 2000)

"Secure System" means computer hardware, software, and procedure that -

: • are reasonably secure from unauthorized access and misuse;

- provide a reasonable level of reliability and correct operation;
- are reasonably suited to performing the intended functions; and
- adhere to generally accepted security procedures.

"Subscriber" means a person in whose name the Electronic Signature Certificate is issued.

CYBER LAW IN INDIA

In India, cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Actis to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

The following Act, Rules and Regulations are covered under cyber laws: •

Information Technology Act, 2000

• Information Technology (Certifying Authorities) Rules, 2000 •

Information Technology (Security Procedure) Rules, 2004

• Information Technology (Certifying Authority) Regulations, 2001 **Need for cyber law in India**

• India has an extremely detailed and well-defined legal system in place. • The existing laws of India, even with the most benevolent and liberal interpretation, could not be interpreted in the light of the emerging cyberspace, to include all aspects relating to different activities in cyberspace.

• None of the existing laws gave any legal validity or sanction to the activities in Cyberspace.

• Internet requires an enabling and supportive legal infrastructure in tune with the times.

Salient features of the Information Technology (Amendment) Act, 2008 i. The term 'digital signature' has been replaced with 'electronic signature' to make the Act more technology neutral.

ii. A new section has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.

iii. A new section has been added to define cyber cafe as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of

the public.

iv. A new definition has been inserted for intermediary.

v. A new section 10A has been inserted to the effect that contracts concluded electronically shall not be deemed to be unenforceable solely on the ground that electronic form or means was used.

vi. The damages of Rs. One Crore prescribed under section 43 of the earlier Act of 2000 for damage to computer, computer system etc. has been deleted and the relevant parts of the section have been substituted by the words, 'he shall be liable to pay damages by way of compensation to the person so affected'.

vii. A new section 43A has been inserted to protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the person so affected.

viii. Sections 66A to 66F has been added to Section 66 prescribing punishment for offences such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism.

ix. Section 67 of the IT Act, 2000 has been amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form to three years from five years and increase the fine thereof from Rs.100,000 to Rs. 500,000. Sections 67A to 67C have also been inserted. While Sections 67A and B deals with penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, Section 67C deals with the obligation of an intermediary to

preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe.

x. In view of the increasing threat of terrorism in the country, the new amendments include an amended section 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource. Further, sections

69A and B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

xi. Section 79 of the Act which exempted intermediaries has been modified to the effect that an intermediary shall not be liable for any third party information data or communication link made available or hosted by him if; (a) The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; (b) The intermediary does not initiate the transmission or select the receiver of the transmission and select or modify the information contained in the transmission; (c) The intermediary observes due diligence while discharging his duties. However, section 79 will not apply to an intermediary if the intermediary has conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act or upon receiving actual knowledge or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by it is being used to commit an unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

xii. A proviso has been added to Section 81 which states that the provisions of the Act shall have overriding effect. The proviso states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

Rules notified under the Information Technology Act, 2000

a) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

b) The Information Technology (Electronic Service Delivery) Rules, 2011

c) The Information Technology (Intermediaries guidelines) Rules, 2011 d) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011 e) The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009

f) The Cyber Appellate Tribunal (Procedure for investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009

g) The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public), 2009

h) The Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009

i) The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

j) The Information Technology (Use of electronic recordsand digital signatures) Rules, 2004

k) The Information Technology (Security Procedure) Rules, 2004

l) The Information Technology (Other Standards) Rules, 2003

m) The Information Technology (Certifying Authority) Regulations, 2001 n) Information Technology (Certifying Authorities) Rules, 2000

CYBER CRIMES / CYBER FRAUDS

The Internet has become a basic fact of everyday life for millions of people worldwide, from e-mail to online shopping. Ever faster and more accessible connections available on a wider range of platforms, such as mobile phones or person to person portable devices, have spurred new e-commerce opportunities. Online shopping and banking are increasingly widespread and over the next 10 years, the Net is expected to become as common as gas or electricity. The invention of the computers has opened new avenues for the fraudsters. It is an evil having its origin in the growing dependence on computers in modern life.

Fraud is the intentional deception of a person or group for the purpose of stealing property or money.

Internet fraud includes any scheme using Web sites, chat rooms, and email to offer nonexistent goods and services to consumers or to communicate false information to consumers. Customers then pay for the fraudulent goods over the Internet with their credit cards. Internet fraud involves a wide variety of schemes limited only by the imagination and creativity of a seller intent on deceiving a buyer. A few general characteristics one can find in all cyber scams. Most scams are done by e-mail. They entice users to give them critical

information like usernames, passwords, credit card information, or other types of account information.

Cyber fraud has the potential of hindering the economic and social development of any nation. This is because among other dire consequences, foreign investment is seriously discouraged. Cyber fraud can also destroy our good and morally sound culture. This is because the youth will no longer work but resort to that means to earn their living.

Types of cyber frauds

A wide variety of scams operate in the online environment, ranging from fraudulent lottery schemes, travel and credit-related ploys, modem and web page hijacking, and identity theft (ID theft) to name but a few. Many of these scams, such as pyramid selling, are simply online variants of fraudulent practices that have long existed offline. However, the Internet has given criminals access to a worldwide base of consumer targets as well as more opportunities to elude enforcement as they need not be in the same country, or even in the same hemisphere, as their victims.

The Internet allows fraudsters to masquerade as legitimate traders behind professional-looking websites or on virtual auction sites to advertise "free" or "bargain" prices, "miracle" products, and "exciting" investment and business opportunities. These deceptive and misleading offers trick unsuspecting consumers into buying goods and services on line which turn out to be far less than promised or even non-existent.

Many online scams originate in spam messages – usually through e-mail, but sometimes through text messages (SMS), voice messages delivered by Internet (Voice-over Internet Protocol or – VoIP) or other electronic channels. Spam has evolved into a vehicle for the spread of fraud and other online abuses. Many e- mail users will have received a message from a person claiming to be a government official or member of the royal family of a foreign country

(usually in Africa), promising substantial sums of money in return for assistance in transferring money out of the country. Commonly known as the "Nigerian", "West African" or "419" scam, once it has sucked in victims it convinces them to make small advance payments for various reasons, such as banking transaction fees. Needless to say, the victim never receives the promised

substantial sums in return. Many pyramid and work-at-home schemes are also distributed through spam and follow the “advance fee fraud” format of requiring up-front payment or investment on the promise of high returns that are never forthcoming.

Spam is a key tool for the spread of ID theft, luring people into disclosing sensitive information such as credit card numbers or passwords. For example, phishing spams falsely claim to come from legitimate and well-known financial institutions or merchants. They ask recipients to click through on hyperlinks in order to verify or update their online accounts. These hyperlinks direct users to fake “look alike” websites where users are tricked into divulging personal information which can be used to access and illegally transfer money out of the victim’s bank account(s), open new bank or credit card accounts in the victim’s name, make unlawful online purchases, etc.

These attacks are continually becoming more sophisticated. The past year has seen the growth of a new practice known as spear-phishing where accurate information about the recipient, such as the full name and home address, is included in the phishing e-mail making it even more convincing. Another new phenomenon known as vishing tricks people into making phone calls rather than clicking on links to websites. The number given is to a VoIP phone which records digits (such as account numbers) entered into the telephone, again enabling crooks to steal and use the information.

Other variants of fraud rely on the use of identity stolen through technological methods. For example, pharming interferes with the domain name system (DNS) look up process and redirects users attempting to reach a particular website to a “spoofed” one where they divulge personal information to the crooks. Malware (or malicious software), can be downloaded unwittingly by consumers from spam attachments or as they surf on line. Such malicious

code, which increasingly targets mobile phones and other portable devices in addition to computers, can install “key stroke” loggers and other programs to steal information stored on, entered into, or received by these devices. The information collected through these kinds of technological attacks, such as passwords and other sensitive data, can then be used to perpetrate fraud.

Preventive measures

The first line of defence to prevent online consumers from becoming online victims is good education. Tips on the major forms of Internet fraud and how to combat them have been developed by public authorities, enforcement agencies, and the private sector on various platforms such as government websites, brochures, posters, videos, reports, etc. The International Consumer Protection and Enforcement Network (ICPEN), an informal network of enforcement authorities from OECD and other countries, has launched Fraud Prevention Month, an awareness campaign taking place on a designated month every year.

The private sector also offers a number of technical tools to provide consumers with real-time protection against cyber fraud. For example, business has developed means to counter spam messages, which are a significant source of fraud, through authentication, filters, and listings. Likewise, anti-phishing systems have been put in place allowing Internet users to report phishing sites and block them.

Preventive measures to be taken to protect their businesses –

- Setup an e-security program for your business.
- Ensure your security program facilitates confidentiality, integrity and availability.
- Identify the sources of threats to your data from both internal and external sources. Examples: disgruntled employees - leaving bugs behind in your system, hackers looking to steal confidential information.
- The security program that you create for your business must have provisions to maintenance and upgrades of your systems.
- Administrators have access to all files and data. Therefore, one must be mindful of who is guarding the guards.

- Roles for security should be defined, documented, and implemented for both your company and external contractors.
- Establish a security awareness program for all users. Content should be communicated in non-technical terms. This could include briefings, posters, clauses in employee contracts, security awareness days etc.
- Implement security training for technical staff that is focused on the security

controls for their particular technical areas.

- Maintain logs of all possible activities that may occur on your system. System records must note who was using the system, when, for how long, deletions etc.
- User accounts should not be shared. User authorization should be mandatory. Employees should only be able to see information that they are authorized to see.
- Employee user accounts must be disabled or removed when no longer needed. Example: in case an employee leaves the company.
- Ensure network security from external sources by installing firewalls and intrusion detection systems.
- Allow remote access to employees only through secure communication channels like SSL or VPN.
- Install antivirus software on all desktops and servers. Buy Anti-Virus software solutions that allow real time upgrading of systems with anti- virus patches. ○ Create a data backup and disaster recovery plan in case of unforeseen natural calamities.
- Ensure back-up procedures are in place and tested.
- Ensure back-up procedures include all the critical as well as back office data such as finance, payroll etc.
- Incident response is the ability to identify, evaluate, raise and address negative computer related security events.
- In case of an incident, do not panic, and continue to save logs.

- Incident response - Take a backup of the affected system and notify the authorities.

The draft National Cyber Security Policy of India has been prepared by CERT- In. The policy is intended to cater to a broad spectrum of ICT users and providers including Government and non-Government entities. Besides this CERT-In in coordination with MHA, NIC and other stakeholders prepared and circulated Computer security guidelines and procedures for

implementation across all Central Government Ministries/Departments.

Cyber crimes and Types

1. Cyber pornography

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). (Delhi Public School case)

2. **Sale of illegal articles:**

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

3. **Online gambling**

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported. Whether these

sites have any relationship with drug trafficking is yet to be explored. Recent Indian case about cyber lotto was very interesting. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name him as the beneficiary of the 12.5 million pound. After confirmation a Telugu newspaper published this as a news. He collected huge sums from the public as well as from some banks for mobilization of the deposits in foreign currency. However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced. Mohan had

pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name. 4.

Intellectual Property crimes

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. In other words this is also referred to as cyber squatting. Satyam

Vs. Siffy is the most widely known case. Bharti Cellular Ltd. filed a case in the Delhi High Court that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. The court directed Network Solutions not to transfer the domain names in question to any third party and the matter is sub-judice. Similar issues had risen before various High Courts earlier. Yahoo had sued one Akash Arora for use of the domain name 'Yahooindia.Com' deceptively similar to its 'Yahoo.com'. As this case was governed by the Trade Marks Act, 1958, the additional defence taken against Yahoo's legal action for the interim order was that the Trade Marks Act was applicable only to goods.

5. **Email spoofing**

A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. Gauri has an e-mail address gauri@indiaforensic.com. Her enemy, Prasad spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e mails appear to have originated from Gauri, her friends could take offence and relationships could be spoiled for life. Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Recently, a branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. Unfortunately this

information proved to be true in the next few days. But the best example of the email spoofing can be given by an Executive's case, where he pretended to be a girl and cheated an Abu dhabi based NRI for crores by blackmailing tactics.

6. Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds

touts soliciting the sale of fake mark sheets or even certificates. These are made using computers,

and high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates. Some of the students are caught but this is very rare phenomenon. **7. Cyber Defamation:**

This occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. India's first case of cyber defamation was reported when a company's employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

The company was able to identify the employee with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

8. Cyber stalking

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

9. Unauthorized access to computer systems or networks

This activity is commonly referred to as hacking. The Indian law has, however, given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking". However, as per Indian law, unauthorized access does occur, if hacking has taken place. An active hackers' group, led by one "Dr. Nuker", who claims to be the founder of Pakistan Hackerz Club, reportedly hacked the websites of the Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nations (India).

10. Theft of information contained in electronic form

This includes information stored in computer hard disks, removable storage media etc.

11. Email bombing

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

12. Data diddling

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems. The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in his bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

13. Salami attacks

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been supposedly mistreated by his employers the man first introduced a logic bomb

into the bank's systems. Logic bombs are programmes, which get activated on the occurrence of a particular predefined event. The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters. Then he went and opened an account in the name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither any of the account holders nor the bank officials noticed the fault.

It was brought to their notice when a person by the name of Zygler opened his account in that bank. He was surprised to find a sizeable amount of money being transferred into his account every Saturday. Being an honest person, he reported the "mistake" to the bank authorities and the entire scheme was revealed.

14. Denial of Service attack

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread.

It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay!

15. Virus / worm attacks

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate. In May 2000, this deadly virus became the world's most prevalent virus. It

struck one in every five personal computers in the world. When the virus was brought under check the true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US $ 10 billion. VBS_LOVELETTER utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses. The e-mail which was sent out had "ILOVEYOU" in its subject line. The attachment file was named "LOVE-LETTER-FOR YOU.TXT.vbs". People wary of opening e- mail attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

16. Logic bombs

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

17. Trojan attacks

A Trojan as this program is aptly called is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

There are many simple ways of installing a Trojan in someone's computer. To cite an example, two friends Rahul and Mukesh (names changed), had a heated argument over one girl, Radha (name changed) whom they both liked. When the girl, asked to choose, chose Mukesh over Rahul, Rahul decided to get even. On the 14th of February, he sent Mukesh a spoofed e-card, which appeared to have come from Radha's mail account. The e-card actually contained a Trojan. As soon as Mukesh opened the card, the Trojan was installed on his computer. Rahul now had complete control over Mukesh's computer and proceeded to harass him thoroughly.

18. Internet time theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In May 2000, the economic offences wing, IPR section crime branch of Delhi police registered its first case involving theft of Internet hours. In this case, the accused, Mukesh Gupta an engineer with Nicom System (p) Ltd. was sent to the residence of the complainant to activate his Internet connection. However, the accused used Col. Bajwa's login name and password from various places causing wrongful loss of 100 hours to Col. Bajwa. Delhi police arrested the accused for theft of Internet time. On further inquiry in the case, it was found that Krishan Kumar, son of an ex army officer, working as senior executive in M/s Highpoint Tours & Travels had used Col Bajwa's login and passwords as many as 207 times from his residence and twice from his office. He confessed that Shashi Nagpal, from whom he had purchased a computer, gave the login and password to him. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cyber crimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested Krishan Kumar under sections 379, 411, 34 of IPC and section 25 of the Indian Telegraph Act. In another case, the Economic Offences Wing of Delhi Police arrested a computer engineer who got hold of the password of an Internet user, accessed the computer and stole 107 hours of Internet time from the other person's account. He was booked for the crime by a Delhi court during May 2000.

19. Web jacking

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website. In a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail.

It was three days later that she came to know, following many telephone calls from all over

the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'. In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured!

20. Theft of computer system

This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

21. Physically damaging a computer system

This crime is committed by physically damaging a computer or its peripherals. This is just a list of the known crimes in the cyber world. The unknown crimes might be far ahead of these, since the lawbreakers are always one-step ahead of lawmakers.

Who commits cyber crimes?

i. Insiders - Disgruntled employees and ex-employees, spouses, lovers ii.
Hackers - Crack into networks with malicious intent
iii. Virus Writers - Pose serious threats to networks and systems worldwide iv. Foreign Intelligence - Use cyber tools as part of their Services for espionage activities and can pose the biggest threat to the security of another country
v. Terrorists - Use to formulate plans, to raise funds, propaganda