CYBER SECURITY IN INDIA: AN ANALYSIS

Dr. Manjit Singh, Assistant Professor, Department of Laws, Guru Nanak Dev University, Amritsar.

Kamni Sharma, Assistant Professor, Punjab College of Law, Usma, Tarn Taran.

Rather than fearing or ignoring cyber-attacks, do ensure your cyber security to them.[1]

ABSTRACT:

The present chapter makes a humble attempt to study the concept of cyber security. Cyberspace is not a new phenomenon in the overall world. Electronic messages reside in cyberspace, a virtual environment where they are conveyed from one computer to another. Technology makes life easier for people, but it also puts their privacy at danger. At present scenario, mostly people depend upon the digitization system because under the umbrella of digital India everyone accesses the electronic way and fills out the information without thinking it and this thing is a chance to the attackers who wait for this moment. They gather the details of innocent people and use it for their own purpose and make money from it. To solve these kinds of things, the concept of cyber security came into existence. Cyber security is a process in which details of the user are protected against the Cyber attackers. This research looks into several aspects of cyber-attacks. The research paper starts with the concept of introduction, real meaning of cyber security, kinds and reasons of need the concept of cyber security. It also covers the legal provisions which are protecting the data under cyberspace and curbing the issue of cyber-attacks.

Keywords: Cyber security, Information Technology, Virus, Cyber Attackers etc.

[1] Available at: https://www.goodreads.com/quotes/tag/cyber-security (last visited on 15 November 2024).

1. **Introduction:** Digital platform is a recent trend which is mostly used all over the world. People more frequently used digital media for each and every purpose. For example - Digital marketing, campaign, even digital payment. Especially, today's era of e- commerce. E-commerce is achieving tremendous growth in the past years. Through the electronic commerce all the goods and services, trade and commerce came into the door of the buyer and seller. But where technology provides comfort to society, it also leaks the private information of the people who used these technologies. The annual number of data breaches is rising as the global cyber threat rapidly evolves. The governmental sector, retail, and medical industries experienced the highest number of breaches and criminals were typically to blame. Cybercriminals are more interested in certain businesses than others because they collect financial and health-care data, but any company that uses networks could be the victim of customer attacks, intellectual property theft, or data theft. Cyber security is a challenge to the attackers who attack the network systems and use the data of people for earning purposes.

2. **Cyber Crime:** In the digital age, the aspect of cybercrime is nothing new. Since the idea of digitalization has existed, cybercrime has been steadily rising. Any crime carried out on a computer is considered a cybercrime. The definition of cybercrime is "Any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime".[2] It includes both traditional computer-related crimes like theft, fraud, and extortion, as well as computer-specific crimes like email viruses, hacking, and denial of service attacks.[3]

3. **Meaning of Cyber Security:** It is a key which locks the various risk attackers from all over the world. Cyber security is a key which locks the various risk attackers from all over the world. It is a system that protects the details of the user against the unwanted spammers. Cyber security is the process of preventing hostile breaches into computer systems, networks, servers, mobile devices, electronic devices, and data. It is frequently called information technology security or electronic information security. It falls into two categories: security and cyber. Systems, networks, programs, and data are all included in what is known as "cyber." Another aspect of security is the protection of programs, networks, systems, and data. Information technology security, electronic information security, or E-security are other names for it. Its goals are to reduce the risk of cyber-attacks and protect against the misuse of systems, networks, and

[2] Anirudh Rastogi, *Cyber Law* 82 (LexisNexis, Haryana, 2014).
[3] *Id* at 83.

technology. Cyber security is the collection of guidelines and procedures intended to defend our online data and computer resources from attacks. The cyber security involves the following aspects:

- Protecting computer, computer system and computer network;
- Protecting gadgets, products, and software;
- Securing hardware and software, and
- Securing information, data and/or databases[4]

According to the Information Technology Act, 2000: Section 2(1)(nb) of IT Act define the term cyber security" refers to safeguarding data, devices, computers, communication devices, and computer resources from unwanted access, use, disclosure, disruption, alteration, or destruction.[5]

According to Dr VK Saraswat: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[6]

4. **Need of Cyber Security:** We now live in a digital age when software applications, computers, networks, and other electronic gadgets are essential to every part of our life. Cyber security is essential to the information technology industry. One of the biggest challenges facing cyber security analysts is safeguarding user data and information from cybercriminals. The concept of cyber security has come into existence when cyber -crime is increasing day by day in society. On the internet, there is a number of user information which is stored in the server of the government, academic institutions, hospital records which is used by the hackers and this information is misused by them. So, there is a need for security which protects the privacy of the user against hackers.

[4] Vakul Sharma & Seema Sharma, I*nformation Technology Law and Practic*e 19 (LexisNexis, Noida, 7th edition, 2021).
[5] *Ibid.*
[6] Available at: https://www.niti.gov.in (last visited on 16 November 2024).

5. **Kinds of Cyber Security:** The use of technology, procedures, and policies to defend against cyber-attacks on systems, networks, programs, devices, and data is known as cyber security. To reduce the threat of cyber-attacks, cyber security is essential. The collection of tools, procedures, and practices known as cyber security is intended to defend networks, hardware, software, and data against intrusions, theft, alteration, and unauthorized access.[7]

   i. **Network Security:** Network security is the process by which any corporate organization uses both hardware and software measures to safeguard its computer network and data. This aims to preserve the privacy and accessibility of the networks and data. Every business that deals with a lot of data has some sort of security against various assaults. The best example of network security is password protection, which is the most basic kind, in which the user selects the password on their own.

   ii. **Application Security:** It is a type of security instrument that exclusively works with applications, as the name implies. Finding, addressing, and resolving security issues in internal organization applications are its goal. Its sole foundation is the identification and remediation of vulnerabilities linked to deficiencies. Its primary objectives are to improve app security and stop data or code theft or modification. It improves application security, protects private data, stops sensitive information from leaking, and lessens risks from both internal and external sources.[8]

   iii. **Information or Data Security:** Information security refers to the steps taken as a shield of data against unwanted access and usage. Cyber security and Network Security are included in this superset. Every business that handles a significant amount of data needs to be protected to some extent from various online dangers. Unauthorized access, disclosure, modification, and disruption are all targets of cyber attackers. Information security ensures the protection of transit and stationary data.[9]

   iv. **Identity Security:** A complete solution for protecting every identity used within a company is identity security. According to the theory underpinning identity security, any identity whether that of an IT administrator, remote worker, third-party supplier, device, or applications may acquire privileges under particular conditions, opening the door for

[7] Available at: https://www.javatpoint.com/what-is-cyber-security (last visited on 17 November 2024).
[8] Available at: https://www.geeksforgeeks.org/ (last visited on 17 November 2024).
[9] *Ibid.*

assaults against a business's most important assets. Identity protection is therefore necessary. Proper authentication of each identity, granting the necessary permissions to each identity, and giving that identity organized access to financial assets in a way that can be reviewed (or taken into consideration) to ensure the process is sound are all components of a comprehensive identity security strategy.[10]

v. **Operational Security:** It is often known as operational protection, is a risk management method that requires managers to evaluate activities from an adversary's perspective in order to avoid sensitive data from falling into the wrong hands.[11] The sensitive data is identified as part of the operational security process, which also includes financial statements, customer information, employee information, and intellectual property.

vi. **Mobile Device Security:** "Mobile device security" refers to the measures set up to protect private information that is transferred and kept on desktops, laptops, electronic watches, and other types of portable devices. Preventing unauthorized people from accessing the company network is the main goal of mobile device security. It is part of an all-encompassing company security plan. One of the easiest ways to stop unwanted access to a mobile device is to create a strong password for it.

vii. **Cloud Security:** Many businesses are embracing cloud computing these days, where a significant amount of critical data is kept online. A subcategory of cyber security known as "cloud security" is devoted to protecting cloud computing infrastructure. This involves preserving data privacy and security across web-based apps, infrastructure, and platforms. To put it another way, cloud security is the entirety of the protocols, best practices, and technologies that safeguard cloud computing environments, cloud-based apps, and cloud-based data.[12]

6. **Cyber Security in India:** India is seeing a daily rise in cybercrime. Every day, someone receives a message or URL link that claims to offer financial rewards by clicking on it, but each time, innocent individuals fall prey to cybercrime. Cybercriminals utilize a wide range of methods to steal money from website visitors who have entered their login information The IT legislation offers a legal foundation to support any required cybercrime investigation,

[10] Available at: https://www.geeksforgeeks.org/ (last visited on 17 November 2024).
[11] Available at: https://digitalguardian.com/blog/what-operational-security (last visited on 15 November 2024).
[12] Available at: https://www.kaspersky.co.in/resource-center/definitions (last visited on 17 November 2024).

search, and seizure. Organizations like the Indian Data Security Council and the Central Bureau of Investigation have released guidelines in this regard. In view to mitigate the problems of cyber-attacks, the Government of India enforced certain provisions, act and applications which specifically deals with cyber-crimes such as-

A. **Information Technology Act, 2000:** The Information Technology Act of 2000 was passed by the Indian Parliament in that year. It serves as India's main legal foundation for issues relating to e-commerce and cybercrime. The purpose of the Act was to prevent cybercrime, give binding force to online transactions, and advance e-governance. This act established sanctions for offenses involving security breaches, such as destroying computer systems or engaging in cyber terrorism. In 2008, this act was modified. A new clause that explicitly offers protection against cybercrimes was included by this change such as-

i. **Section 43A (Mandates compensation for failure to protect personal data):** Section 43A states that a body corporate, which is a company, firm, or other organization engaged in business-related or professional activities, is responsible for paying damages to anyone who loses money or gains money unfairly because the company failed to put in place sufficient security measures to protect sensitive personal information. This section only gives civil compensation not the criminal punishment to the offender.

ii. **Section 66 (Deals with computer-related offences):** According to section 66 of IT Act, "if any person, dishonestly or fraudulently, does any act referred to in Section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both".[13] In simple words, cybercrimes that involve dishonest or deceptive intentions when executing any of the acts described under Section 43 of the IT Act are covered by Section 66.

iii. **Section 66F (Defines cyber terrorism):** Cyber terrorism, as defined by Section 66F, is when someone uses a computer system to compromise national security, instill fear, harm essential systems, or get private information without authorization in order to weaken or influence a government. Section 66F (2) deals with the punishment which is imprisonment for life and includes the fine also. This is the major offence under the Information

[13] Information Technology Act, 2008, (ITAA 2008), s.66.

Technology Act, 2008. It is non-bailable and cognizable offence.

iv. **Section 69B (Power to authorize, monitor and collect traffic data):** The Central Government gives authorized authorities the authority to monitor and gather traffic information and data through any computer resource for security purposes, as stated in Section 69B of the IT Act of 2000. Additionally, this clause gives the officer the authority to locate and examine the computer system's data and content. For the good of the nation, it also gives the government the authority to prohibit websites. The law also included procedural procedures for prohibiting any website. Recently, some Chinese apps were blocked under Section 69A of the IT Act.

v. **Section 70 (Protected System):** The term Protected System is deals under section 70 of the Information Technology Act, 2000. This clause allows the relevant government to declare any computer resource that has an impact on the Critical Information Infrastructure facility, either directly or indirectly, by publishing a notice in the official gazette. The appropriate government appoints the authorized person who accesses the protected system. Under this clause, anyone who accesses the protected system illegally or without authorization faces a fine and a maximum 10-year prison sentence. The central government also prescribed certain security practices and procedures which are necessary for a protected system.

vi. **Section 70A (National Nodal Agency):** Under section 70A the concept of Nodal Agency is came into existence. The appropriate government appoints any government agency as the National Nodal Agency for the protection of Critical Information Infrastructure under this section by publishing a notification in the official gazette. This nodal organization's mission is to support the country's critical industries by providing reliable, secure, and strong information infrastructure.

vii. **Section 70B (Indian Computer Emergency Response Team):** The Indian Computer Response Team provision is covered under Section 70B of the Act. The Indian Ministry of India's information and communications technology department is home to the Indian Computer Emergency Response Team (CERT-In). Section 70B of the Information Technology Act of 2000, as amended in 2008, states that the Indian Computer Emergency Response Team (CERT-In) is the country's main organization for dealing with cyber threats like phishing and hacking. It acts as the main focus for responding to threats to cyber

security including phishing and hacking. It strengthens the security barriers for the Indian Internet domain. This agency perform the certain functions such as-

a. To gathering information , analysis, and distribution regarding cyber-attacks;

b. To forecast cyber-attacks and warnings;

c. To coordinate with the cyber response activities;

d. To provide guidelines regarding cyber-crime and attacks.

B. **Institutional Framework:** A multi-agency system comprising government ministries, intelligence services, and nodal organizations makes up India's institutional cyber security structure. These organizations are in charge of preventing, keeping an eye on, looking into, and responding to cyber threats in industries like communication, healthcare, energy, defence, and finance. There are certain frameworks which deals to curb the problem of cybercrime such as-

a. National Cyber Coordination Centre (NCCC): The Ministry of Electronics and Information Technology (MeitY) is home to the government organization known as the National Cyber Coordination Centre (NCCC). It acts as a centralized body for monitoring internet activity in India and providing various intelligence and law enforcement agencies with the most recent information on cyber threats. The NCCC is run by MeitY and is not governed by a separate legislative act; rather, it is empowered by the IT Act of 2000. Internet service providers (ISPs) work with NCCC through a Public-Private Partnership (PPP). It ensures a certain degree of privacy compliance by gathering raw data (metadata) rather than content.

b. National Cyber Security Policy, 2013: On July 2, 2013, the National Cyber Security Policy (NCSP) 2013 was released by the Ministry of Communications and Information Technology (Department of Electronics and Information Technology, DeitY. This approach served as the Indian government's first formal framework for defending the nation's digital infrastructure against cyber-attacks. It was India's initial move in the direction of a safe online environment. One of the policy's key goals is to improve the administrative and legal framework for cyber security.

c. **Defence Cyber Agency (DCA):** One of the three tri-service organisations established by the Indian government under the Integrated Defence Staff (IDS) to address cyber threats is the Defence Cyber Agency (DCA). It was formally implemented in May 2019 and operates under the Ministry of Defence (MoD). In the military sphere, it is responsible for enhancing India's cyber warfare capabilities, both offensively and defensively.

d. **Cyber Crime Portal:** The Government of India launched a cybercrime webpage to collect online reports of cybercrime. This portal's name is National Cyber Crime Reporting Portal. The focus of this portal is on women and children who are victims of cybercrime. The goal of this initiative is to offer cyber security to online crime victims. This portal also provides a helpline number that is 1930.

e. **Cyber awareness and hygiene for Institutions:** All of the technical institutions in the nation should observe "Cyber Jaagrookta Diwas" on the first Wednesday of every month to raise awareness of cybercrimes and preventative actions. It holds institution-level cyber awareness training on recommended topics.

   - Cyber security and Crime;
   - A concept and application of online safety;
   - An introduction to social networks Protections for electronic payments.

7. **Conclusion:** These days, the internet is a part of our daily lives. A key component of disseminating knowledge about combating cybercrime is education. Child pornography, rape material, digital stalking, cyber bullying, cyber harassment, and other cybercrimes that specifically target women and children are on the rise as more people use the internet. To defend oneself from these types of online crimes, one should adhere to cyber security principles and protocols. In addition to preventing and addressing cyber threats, the Indian Computer Emergency Response Team (CERT-In) strives to improve the efficacy of cyber security in the country. Cyberspace must be safe and robust in order for India to achieve its goal of turning into a digital giant. Even while legislation and institutional arrangements have advanced, stronger action is still needed to handle the changing threat scenario. Cyber

security requires a multifaceted approach because it is not only a technical problem but also governance, legal, and socioeconomic one.