IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

The Evolving Threat Of Cyber-crime: Trends, Challenges And Solutions

Dr. Wanrishisha Dkhar
Assistant Professor
The Shillong Law College, Shillong
Meghalaya, India

Abstract

Cybercrime has emerged as a significant, pervasive and insidious threat to individuals, organizations, and societies worldwide. The rapid growth of the internet and its online threats and the increasing reliance on digital technologies have created new opportunities for cybercriminals to exploit vulnerabilities and commit crimes. This paper provides an overview of the current state of cybercrime including its types, trends, and challenges. The impact of cybercrime on individuals, property, Government and the economy, as well as the efforts being made to prevent and combat cybercrime has been discussed. A framework for addressing cybercrime which includes relevant provisions of law and case laws has been examined.

Keywords:

Cybercrime, cyber security, online threats, digital technologies, law enforcement, international cooperation.

INTRODUCTION

Cyber-crime originally comes from the ancient Greek word "Kubernetikos" which means "good at steering on piloting". It morphed in French to Cybernetics meaning "the art of governing". With this definition the word Cyber-crime began to resemble its modern form.

But it was the mathematician and the writer "Nobert Wiener" who pushed Cyber closer to everyday use with his 1948 book about cybernetics, or how people, animals and machines control and communicate information.

Cyber-crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic wrecking to denial of service attacks. It is a general term that covers crimes like Phishing, Credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat

rooms, scams, cyber terrorism, creation and distribution of viruses and so on.

It also covers that traditional crimes in which computers or networks are used to enable the illicit activity. Cyber-crimes is increasing day by day, nowadays it has become a new fashion to earn money by fraud calls or take revenge through other accounts.

Cyber-crime encloses a wide range of activities, but these can generally be divided into two categories: -

1) Crimes that aim at computer networks or devices. These types of crimes involve different threats (like virus bugs etc.) and denial-of-services (DOS) attacks.

2) Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Today there are many disturbing things happening in Cyberspace. Due to anonymous nature of the internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the internet to perpetuate criminal activities in cyberspace. Hence, the need for Cyber-laws in India.

ORIGIN OF CYBER-CRIME

Cyber-crime has its origin in the early days of computing and the growth of the internet. The term "Cyber-crime" encompasses a wide range of illegal activities conducted in the digital realm. Some key milestones in the origin of cyber-crime includes: -

1) (1960s-1970s) - The early days

- In the 1960s and 1970s, computers were primarily used in research and academic.
- Early "hackers" like MIT's Tech Model Railroad Club explored computer system out of curiosity, often to improve system functionality.
- The term "hacker" had a positive connotation at this age.

2) 1980s – The Hacking - emergency of Malicious

- The term "hacker" started to take on negative connotations as individuals used their skills for malicious purposes.
- The first computer viruses, like the EIK cloner in 1982, began to appear.
- The Morris worm in 1988 became one of the first major incidents of a self-replicating computer worm that disrupted thousands of computer.

3) 1990s – The Internet Era

- With the growth of the internet, Cyber-crime expanded rapidly.
- Activities included credit card fraud, identity theft and online scams.

- The term "Cyber-crime" gained prominence.

4) Early 2000s – new threat arise

- Distributed denial of service (DDOS) attacks, where multiple compromised computers flood a target with traffic, became a significant threat.
- Phishing schemes, designed to trick individuals into revealing personal information, gained popularity.
- Notable Malware incidents like Code Red and Nimda caused wide – spreads disruptions.

5) Mid 2000s – Organized Cyber-Crime

- Cybercrime became more organized, with criminal groups specializing in various activities.
- Data breaches, where sensitive information was stolen from organizations, grew in scale and frequency.
- Ransom attacks, where data is encrypted and held for ransom, became a major concern.

6) 2010s – High profile breaches and nation state attacks

- Several high-profile data breaches, including target and Equifax exposed the vulnerability of large organizations.
- Nation-state sponsored cyber-attacks, such as the stuxnet worm targeting Iran's nuclear program, highlighted the involvement of Governments in Cyber Espionage.

7) Present – ongoing evolution

- Cyber-crime continue to evolve with advanced hacking techniques, including zero-day exploits.
- The dark web facilities, the buying and selling of illicit goods, services and data, making it harder to track Cyber-criminals.
- Emerging threat include supply-chain attacks, Al driven attacks and increase Cyber-espionage activities.

The Origin of Cyber-crime reflects the parallel growth of technology and illicit activities in the digital realm. As technology advances, cyber-criminals adapt and innovate, posing ongoing challenges Cyber-security, professionals and organizations.

Cyber-crime in India like many other countries, has evolved with the growth of the internet and Digital technologies. The concept of Cyber-crime in India can be traced back to the late 1990s when the internet began to gain popularity. With the increase use of online banking and E-commerce, Cyber frauds became more prevalent. In 2008 India enacted the Information Technology (Amendment) Act, which provided a legal framework to address Cyber-crimes more effectively. It defined various cyber offenses and penalties for those convicted. The 2010s witnessed a significant increase in cybercrime activities in India. Notable incidents include the 2016 data breach at Indian banks and the 2017 want to cry ransom ware attacks. Cyber criminals in India began adopting more sophisticated tactics, such as ransom ware attacks, where they encrypt data and demand a ransom for its release. The 2020s continue to present challenges in the realm of cyber-crime in India. The country had faced an increasing number of Cyber threats, including advanced phishing campaigns related to Covid-19 online frauds and data breaches.

The origin of Cyber-crime in India closely mirror the global trend, with cyber criminals adapting to technological advancements. As the digital landscape continues to evolve, addressing cybercrime remains a priority for law enforcement and cyber-security agencies in the country.

TYPES OF CYBER-CRIME

- **DDoS Attacks (Distributed Denial-of-service):** DDoS attacks are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.
- **Botnets:** Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.
- **Identity Theft:** This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.
- **PUPS:** PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.
- **Online Scams:** These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

CYBER-CRIME AGAINST INDIVIDUAL / PERSONS

Cyber-crime continues to rise in scale and complexity, affecting essential services, business and private individuals alike. Cyber-crime causes untold damage and threaten many individuals. Cyber criminals may attack individuals through computers or electronic networks and individuals anywhere are increasingly becoming targets for Cyber Criminals. Cyber-criminal activity involves an information technology infrastructure including illegal access, illegal interception, data interference, system interference, misuse of device and electronics fraud. Our increased dependence on ICT (Information & Communication Technologies) and the pervasive interconnectivity of our ICT infrastructure exposes us to an evolving spectrum of Cyber-threats.

Securing our network against cyber threats can be challenging, but taking care of the basics can go a long way towards keeping hackers out. Cyber-crimes may affect individuals in different manners like e-mail spoofing, spamming, cyber defamation, phishing, cyber stalking, cyber bullying.

1) **E-mail Spoofing:** - It refers to e-mail that appears to originate from one source but actually has been sent from another source. For example: - Mr. X has an e-mail address x25@gmail.com and his enemy Mr. Z spoofs his e-mail and sends obscene message to all his acquaintances. Since e-mail appears to have originated from Mr. X, his friends could take offence and relationships could be compromised. It involves the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

2) **Spamming:** - Spam is unsolicited commercial sent electronically, usually to most of the people at once, often through mail. Spam generally contains advertising in one or more forms such as offers to sell prescription drugs, stock tips, links to online dating services, pornography websites or various business opportunities often of questionable legitimacy. A person who sends spam is called a spammer. Spam is also associated with distribution of malware such as viruses and Trojans. So it is not only an annoyance to the victim but it may also carry malicious code with it by which the computer or computer network of a victim may get corrupted or damaged.

3) **Cyber Defamation:-** Cyber defamation is an injury done to the reputation of a person published online that may be carried out through emails, social media, spread of malicious gossip on discussion groups or posting of offensive content against a person on a website. There are two types of Cyber Defamation:

(a) Libel and (b) Slander

(a) Libel: - it refers to any defamatory statement published in written form. For instance writing defamatory comments on posts, forwarding defamatory messages on social media groups, etc. are a part of Cyber defamation in the form of Libel.

(b) Slander: - it refers to any defamatory statement published in oral form. For instance, uploading videos, defaming someone on YouTube is a part of cyber defamation in the form of Slander.

4) **Phishing: -** it refers to the fraudulent practice of sending an email to users falsely claiming to be established legitimate enterprise in an attempt to scam the user into surrendering the private information that will be used for identity theft. The term Phishing arises from the use of increasingly sophisticated hires to 'fish' for users finished information and passwords. The term "phishing" is commonly believed to have been derived from the old expression, "Let's go fishing to see what's biting." In the technological world of Cyber-crime, phishing by analogy means to cast "digital bait" on to the internet to see who will bite. Thus, phishing is a type of social engineering that cyber criminals use when attempting to clause potential victims into revealing confidential information about themselves or their computer accounts such as usernames, passwords and financial or bank account numbers. The damage caused by phishing ranges from loss of access to e-mail to substantial economic loss. This style of identity theft is becoming more popular because of the ease with which unsuspecting people after divulge personal information to phishers, including credit card numbers and social security numbers.

5) **Cyber stalking : -** It can be defined as the repeated acts of harassment or threatening behavior of the cyber-criminal towards the victim, by using internet services such as following the victims, making harassing phone calls, vandalizing victims property, leaving written messages or objects.

- In cyber stalking criminals target victims in three areas: - Live chat or Internet Relay Chat (IRT): - In which a user talks live online with other users.
- Message boards and newsgroups: - A user interacts with others by posting messages, conversing back and forth.
- Email Boxes: - A user can write anything or even attach files to the email. Sending electronic viruses, sending unsolicited e-mail and electronic identity theft are quite common manifestations of cyber stalking.

6) **Cyberbullying: -** The term cyberbullying is not defined under any Indian law. However, in general parlance cyber bullying refers to bullying someone by threatening, harassing or embarrassing the victim using technology digital service. Generally, cyberbullying includes the following activities: -

- Humiliating content posted online about the victim.
- Hacking social media accounts.
- Posting vulgar messages on social media.
- Threatening the victim to commit any violent activity.
- Child pornography or threatening someone with child pornography.

CYBER-CRIME AGAINST PROPERTY

This involves damaging or stealing of persons or an organisations property such as malware ransom ware or piracy. Cyber-crime against organisations this involves attacking an organisations network system or data such as denial- of -services, espionage or sabotage.

This classification of cyber-crime includes other kinds of property as well like stealing or destroying intellectual property. Attacks that target your computer itself also fit into the categories. However, any online activity which basically offence human sensibility can be regarded as a cyber-crime against property.

CYBER-CRIME AGAINST GOVERNMENT

It is a global issue that possess significant threads to National security critical infrastructure and the proper functioning of government institutions. Such crimes can target government at various levels including National State Local or even International bodies. Examples of cyber-crimes committed against the government in India are:

- **Hacking and data breaches:** Cybercriminals attempt to gain unauthorized access to government networks data basis or systems to steal sensitive information, disrupt operations or compromise the integrity of government functions. These attacks can expose classified or confidential data including national security information or personal information or government officials and employees.
- **Distributed denial of service attacks**: Hackers launch DDOS attacks against government websites or online services to overwhelm their services with an excessive amount of traffic causing them to slow down or become inaccessible. This disrupts government services, affect citizen engagement and damages the reputation of government institutions.
- **Ransom ware attacks:** Cyber criminals use ransom ware to encrypt government system and data making them inaccessible unless ransom is paid. These attacks can paralyze government operation leading to significant financial losses and potential breaches of national security.

The Government of India has recognized the seriousness of cyber-crimes against the government and has taken initiative to strengthen cyber security measures. This includes establishing the national cyber-crime reporting portal to enable citizen to report incidence and to streamline the process of investigation and prosecution. Additionally the government has invested in training programs partnership with international organisations and the development of national cyber security strategy to enhanced security capabilities and protect government infrastructure and data.

THE INFORMATION TECHNOLOGY ACT, 2000

Meaning of cyber law: Cyber law also called IT law is the law regarding information technology including computers and the internet is related to legal informatics and supervisors the digital circulation of information, software information security and e- commerce.

Significance of Cyber law

- **Protecting individuals and business:** Cyber Laws establish a legal framework to safeguard individual business and organisations from various online threads such as hacking data breaches, identity theft and cyber bullying.
- **Safeguarding privacy:** These laws help protect the privacy of individuals by regulating how personal information is collected, stored and shared online. They also ensure that data breaches are reported and manage appropriately.
- **Intellectual property protection:** Cyber laws play a crucial role in safeguarding intellectual property rights in the digital realm including copyright, trademark and patent.
- **National security:** These laws contribute to national security efforts by addressing cyber terrorism, cyber surveillance and others cyber threats that can disrupt crucial infrastructure and harm the nation interests.
- **Consumer protection:** They ensure that consumers are protected from fraudulent online schemes, misleading advertising and unsafe products or service sold on the internet.

Cyber law is important because it touches almost all aspects of transaction and activities and on involving the internet worldwide web and cyber space. Every action and reaction in cyber space has some legal and cyber legal angles.

HISTORICAL BACKGROUND

On October 17th 2000, The Information Technology Act, 2000 came into effect. This Act extend to the whole of India and its provision also apply to any violation or offence committed by any individual regardless of nationality even outside the Republic of India's territorial authority. Such an offence or contravention shall include a computer system or computer network located in India i.e, subject to the provision of this Act. The extra territorial applicability of the provision of the IT Act is provided by Section 1 (2) read in conjunction with Section 75.

The Information Technology Act of 2000 in India has made effort to include legal ideas found in other Information Technology related laws that have already been passed in other nations as well as different Information Technology law related guidelines. The Act recognizes electronic signature and grant electronic contracts legal validity. Defamation, hacking, data theft, pornography, child pornography, and cyber terrorism are now all considered crime under this modern legislation.

DRAWBACKS OF CYBER-CRIME IN INDIA

Cyber-crime in India has several drawbacks including:

- **Financial loss**: Individuals and business incur substantial financial losses due to Cyber-attacks, including theft of sensitive information, ransom payment and costs associated with recovering from cyber incidents.
- **Data breaches**: Data breaches are a major concern. Cyber-criminals often target databases resulting in the exposure of sensitive information. This can have long- term consequences for affected individuals, including the risk of identity theft and financial fraud.
- **Identity theft:** Stolen personal information can be used for identity theft, which may involve taking out loans or making purchases in the victim's name. Victims often face the arduous task of proving their innocence and resolving financial issues.
- **Privacy violation**: Individual's privacy is compromised when Cyber-criminals gain unauthorized access to their personal devices or online accounts. Private photos, messages and personal information can be exposed, leading to emotional distress and potential blackmail.
- **National Security Risks**: Cyber-attacks on initial infrastructure, government systems, or defense establishments can pose significant national security risks. These attacks may lead to theft of classified information or disrupt essential services.
- **Legal Challenges**: Investigating and prosecuting cyber-crimes can be complicated. Jurisdictional issues arise when cybercriminals operate from other countries. Additionally, the fast-evolving nature of cyber threats makes it challenging for law enforcement agencies to keep up.
- **Lack of awareness**: Many individuals and organisations in India may not be sufficiently aware of cyber security best practices. This lack of awareness can lead to poor security making them more vulnerable to cyber-attacks.

Addressing these drawbacks, requires a multi-faceted approach, including strengthening cyber security infrastructure, educating the public and business on cyber security best practices, enhancing international cooperation to combat cybercrime and continually updating law and regulations to address evolving cyber threats effectively.

PREVENTION OF CYBER-CRIME

With the growth of internet and the services provided the lives of citizens are being transformed and are being empowered through it. However, with the growth of internet there is also an increase in the growth of Cyber-crime.

To prevent cyber-crime successfully, arrange multifaceted public private cooperation among law enforcement organization, the Information Technology Industry, Information security Organization, etc. The regular way altercation of the crime cannot be applied against theses cyber criminals because they do their work together to enhance their chances and they have each other's back.

Given below are some of the ways to prevent Cyber-crime: -

- **Use strong password**: - One of the easiest way to prevent cyber-crime is to use strong password by combining alphabets, numeric and fonts over simple passwords such as 1234… that are easy to guess.
- **Keeping your software updated**: - Keeping and checking the updates for operating systems and internet security keeps your software a step closer from preventing cyber-crime.
- **Keep social media private**: - The next thing that can be done is keep your social networking site private by making sure to lock it down from public eye.
- **Strengthening your network**: - When you use a Wi-Fi use a strong password to protect your home network from unwanted ambush and hackers.
- **Keep up-to-date on major security breaches**: - If you have an account always change your passwords to prevent from any incident where the hackers could get access to your data.
- **Protect yourself from phishing**: - When it comes to phishing learn to recognize it. They prompt you with your greed to act immediately to claim profitable reward and so on. Therefore, be extra cautious when you receive such mails from an unknown person.

CASES REGARDING CYBER-CRIME

Syed Asifuddin and Ors. v. State of Andhra Pradesh and Anr, (2005)

Facts: The subscriber purchased a Reliance handset and Reliance mobile services together under the Dhirubhai Ambani Pioneer Scheme. The subscriber was attracted by better tariff plans of other service providers and hence, wanted to shift to other service providers. The petitioners (staff members of TATA Indicom) hacked the Electronic Serial Number (hereinafter referred to as "ESN"). The Mobile Identification Number (MIN) of Reliance handsets were irreversibly integrated with ESN, the reprogramming of ESN made the device would be validated by Petitioner's service provider and not by Reliance Infocomm.

Questions before the Court:

i) Whether a telephone handset is a "Computer" under Section 2(1)

(i) of the IT Act?

ii) Whether manipulation of ESN programmed into a mobile handset amounts to an alteration of source code under Section 65 of the IT Act?

Decision:

(i) Section 2(1)(i) of the IT Act provides that a "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. Hence, a telephone handset is covered under the ambit of "computer" as defined under Section 2(1)(i) of the IT Act.

(ii) Alteration of ESN makes exclusively used handsets usable by other service providers like TATA Indicom. Therefore, alteration of ESN is an offence under Section 65 of the IT Act because every service provider has to maintain its own SID code and give its customers a specific number to each instrument used to avail the services provided. Therefore, the offence registered against the petitioners cannot be quashed with regard to Section 65 of the IT Act.

Shreya Singhal v. UOI, 24th March, (2015)

In the instant case, the validity of Section 66A of the IT Act was challenged before the Supreme Court.

Facts: Two women were arrested under Section 66A of the IT Act after they posted allegedly offensive and objectionable comments on Facebook concerning the complete shutdown of Mumbai after the demise of a political leader. Section 66A of the IT Act provides punishment if any person using a computer resource or communication, such information which is offensive, false, or causes annoyance, inconvenience, danger, insult, hatred, injury, or ill will.

The women, in response to the arrest, filed a petition challenging the constitutionality of Section 66A of the IT Act on the ground that it is violative of the freedom of speech and expression.

Decision: The Supreme Court based its decision on three concepts namely: discussion, advocacy, and incitement. It observed that mere discussion or even advocacy of a cause, no matter how unpopular, is at the heart of the freedom of speech and expression. It was found that Section 66A was capable of restricting all forms of communication and it contained no distinction between mere advocacy or discussion on a particular cause which is offensive to some and incitement by such words leading to a causal connection to public disorder, security, health, and so on.

In response to the question of whether Section 66A attempts to protect individuals from defamation, the Court said that Section 66A condemns offensive statements that may be annoying to an individual but not affecting his reputation.

However, the Court also noted that Section 66A of the IT Act is not violative of Article 14 of the Indian Constitution because there existed an intelligible difference between information communicated through the internet and through other forms of speech. Also, the Apex Court did not even address the challenge of procedural unreasonableness because it is unconstitutional on substantive grounds.

SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra, (2001)

Facts: In this case, Defendant Jogesh Kwatra was an employee of the plaintiff's company. He started sending derogatory, defamatory, vulgar, abusive, and filthy emails to his employers and to different subsidiaries of the said company all over the world to defame the company and its Managing Director Mr. R K Malhotra.

In the investigations, it was found that the email originated from a Cyber Cafe in New Delhi. The Cyber cafe attendant identified the defendant during the enquiry. On 11th May 2011, Defendant was terminated of the services by the plaintiff.

Decision: The plaintiffs are not entitled to relief of perpetual injunction as prayed because the court did not qualify as certified evidence under section 65B of the Indian Evidence Act. Due to the absence of direct evidence that it was the defendant who was sending these emails, the court was not in a position to accept even the strongest evidence. The court also restrained the defendant from publishing, transmitting any information in the Cyber space.

Poona Auto Ancillaries Pvt. Ltd., Pune Versus Punjab National Bank, HO New Delhi & Others, (2013).

Summary: In 2013, in one of the largest compensation awarded in legal adjudication of a cyber-crime dispute, Maharashtra's IT secretary Rajesh Aggarwal had ordered PNB to pay Rs 45 lakh to the Complainant Manmohan Singh Matharu, MD of Pune-based firm Poona Auto Ancillaries. A fraudster had transferred Rs 80.10 lakh from Matharu's account in PNB, Pune after Matharu responded to a phishing email. Complainant was asked to share the liability since he responded to the phishing mail but the Bank was found negligent due to lack of proper security checks against fraud accounts opened to defraud the Complainant.

CHRISTIAN LOUBOUTIN SAS Versus NAKUL BAJAJ & ORS (Intermediary Liability as an E-commerce Operator – November 2018)

Great analysis of section 79 of IT Act, 2000 and the Intermediary Guidelines done by honorable Judge Ms Pratibha M Singh. Importantly, it lays down the circumstances, in which the Intermediary will be assumed to be abetting the sale of online products/services and therefore, cannot go scott free. In the said matter, the Complainant, a manufacturer of Luxury Shoes filed for injunction against an e-commerce portal www.darveys.com for indulging in Trademark violation, along with the seller of spurious goods.

CONCLUSION

Financial frauds accounted for over 75 per cent of cyber crimes in the country from January 2020 till June 2023, with nearly 50 percent cases related to UPI and internet banking, according to a new study by an IIT Kanpur-incubated start-up. When we look at Social media-related crimes such as cheating by impersonation, cyber-bullying, sexting and email phishing accounted for 12 per cent of the online offences during the period, according to the study. "This category encompasses a wide range of crimes associated with online platforms and social media. Subcategories within this domain include cheating by impersonation, cyber-bullying, sexting, email phishing, and more. While cyber-bullying and impersonation accounted for significant percentages, email phishing and provocative speech for unlawful acts had a comparatively lower impact,"

The FCRF stated that "other notable categories" contributed to nine per cent of the online crimes which delve into several other cybercrime categories with smaller but notable percentages, including online cyber-trafficking, online gambling, ransom ware, crypto currency crime, and cyber terrorism.

Therefore, it is of critical importance to ensure global cooperation through information sharing and strengthening joint efforts in cyber security research and development as most cyber-attacks originate from beyond the borders. And for the corporates or the respective government departments to find the gaps in their organisations and address those gaps and create a layered security system wherein security threat intelligence sharing is happening between different layers.

References:-

1. The Information Technology Act, 2000
2. Nilakshi Jain, Ramesh Menon, (2020), Cyber Security and Cyber Laws, Wiley India Pvt Ltd
3. Debtoru Chatterjee, (2020), Cyber Crime And Its Prevention In Easy Steps, Khanna Book Publishing Co.(P) LTD
4. Dr Santosh Kumar, (2021),Cyber Laws and C rime, Whitesmann Publishing Co.
5. Talat Fatima, (2024), Cyber Crimes, Eastern Book Company
6. Heena.T.Bhagtani, (2017), Cyber Crimes And Cyber Security, Himalaya Publishing House.
7. https://www.legalserviceindia.com
8. https://infosecawareness.in/cyber-lawsofindia
9. https://www.csk.gov.in
10. https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/?amp=1
11. https://blog.ipleaders.in
12. https://www.cybersecurityintelligence.com
13. https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an- overview.html
14. https://www.itlaw.in/judgements/
15. https://www.hindustantimes.com/