INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 3 - V7I3-2157)
Available online at: https://www.ijariit.com

Why India is an easy target for Cybercriminals?

Ravichandran Ramasamy
lionravichandran@gmail.com
Livingstone International University of Tourism Excellence and Business Management, Lusaka, Zambia

ABSTRACT

The proliferation of newly developed technologies is a boon to society. At the same time, it showed the way for new types of technological crimes, particularly cybercrimes. In recent years, cybercrime becomes one of the greatest threats to humanity. Safeguarding against cybercrime is a vital part of every government. Cybercrime could be originated from any part of the world, crossing the international boundaries over the internet resulting in damages to the governments, organizations, and public. The technical and legal complexities of investigating and prosecuting these crimes are the foremost task for law enforcement agencies. Cybercrime is the most common threat for financial markets. Cyber-attacks have already caused considerable damage to retail banking, mainly through payment card scams and cyber frauds. In India, the Information Technology Act and its associated Rules and Regulations deal with cybersecurity and cybercrimes. Other laws contain some of the provisions of cybersecurity protection are the Indian Penal Code 1860 (IPC), and the Companies (Management and Administration) Rules 2014. But none of these laws is a dedicated cybersecurity law. Some sector-specific regulations like the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India (IRDA), the Department of Telecommunication (DOT), and the Securities Exchange Board of India (SEBI) have mandated their respective entities to adhere to cybersecurity standards prescribed by the regulators. The long wait Data Protection Act with international perception is yet to be released. However, we need to fight against cyber criminals effectively to cope up with the international requirements. The salient purpose of this article is to find implementable solutions to curtail the growing menace of cybercrimes in India.

Keywords— *Cyber Laws, Cybercrime, Cybersecurity, Cybercriminal, Cyber-Attacks, Cyber-Frauds, Information Technology Act, Computer Crime*

1. INTRODUCTION

When I came across a piece of cyber-sabotage news [1] that a Chinese Government sponsored group of cybercriminals have caused a power outage- in Mumbai on October 13, 2020, my thought process started asking why India is the easy target for cybercriminals. Many historical precedents present that India has been attacked many times by state-sponsored cyber espionage. [2]

India is the second-largest consumer market and a country with one of the largest bases of online consumers, often vulnerable to several national and international cyber-attacks. As India has been steadily inching towards a technology-enabled economy by utilizing emerging technologies like Artificial Intelligence (AI), Machine Language (ML), Internet of Things (IoT), etc., International statistics show cyberattacks are prevalent against Indian industries and individuals, including hacking, spam, virus, credit card fraud, trafficking, pornography, posting an obscene photograph, and sending fake emails to get personal information, misusing personal data, digital piracy, money laundering, counterfeiting, altering data for either profit or political objectives, violating privacy by stealing identity and many more.

Microsoft, an international software giant, has conducted a study in India and revealed that 53% of Indian children are bullied online. [3] Many children even commit suicide when their offensive pictures are posted online. Daily news on defacement of websites (Web defacement is an attack in which malicious hackers penetrate a website and replace content on the site with their messages) [4] and security incidents of phishing (Phishing is a process of trying to gather personal information using deceptive emails and websites).[5] Virus spread amounting to a ransomware attack is increasing at an alarming rate.

India has developed cyber laws to deal with this situation in 2000, known as Information Technology Act, 2000 [6], and updated with some amendments in 2008. Many cybersecurity standards and guidelines were framed and published for the use of organizations to combat cybercrime proactively. Information Technology Act (IT Act) provides protection for transactions carried out through electronic data interchange and other means of electronic communication, contains provisions safeguarding electronic data, information, or records, and preventing unauthorized or unlawful use of a computer system.

"The Indian IT Act is not a cybersecurity law and therefore does not deal with the nuances of cybersecurity," explains Dr. Pavan Duggal, Advocate, Supreme Court of India [7]. In India, most cyber-crime cases are committed by educated persons. Also, in India, most of the issues are crimes committed due to lack of knowledge or by mistake.

At this juncture, questions arise. Why is India an easy target for cybercriminals? Whether is India capable of tackling the ill effects of these sophisticated cybercrimes?

2. EVOLUTION OF CYBERCRIME

Aristotle, the legendary Greek philosopher, told "Man is by nature a social animal. Everyone owes certain duties towards his fellow men and enjoys certain rights and privileges entrusted to him. Though most people are duty-bound and law-abiding, very few, for some or other reasons, deviate from the usual behavioral pattern. The conduct and behaviors prohibited under the existing law at a given time and place are known as wrongful acts or crimes, while those permitted under the law are treated as lawful. The wrongdoers are punished for their guilt under the direction of the land.

Computer systems are being used extensively every day and everywhere, particularly in industries, businesses, public authority, military, police, scientists, technologists, and worldwide. Computers are a great boon to society. Nevertheless, they have also been subjected to abuse by criminals to perpetrate their crimes with ease and tremendous immunity from punishment or recrimination. Any coin has two sides, the same for cyberspace, its advantages, and disadvantages, and one of the most significant disadvantages is cybercrime. With the development of technological resources, particularly electronic data processing, used in the business world, a new type of crime has arisen, called cybercrime. Cybercrime is the latest and perhaps the most complicated problem in this modern world.

There is no distinction between cybercrime and conventional crime. However, on deep introspection, we may say that there exists a hairline of distinction between conventional and cybercrime, which lies in the involvement of the medium in cases of cybercrime. The complexity of cybercrime is based on two prominent differences it has with ordinary crime. Firstly, the criminal does not have to be at the crime scene to commit the act. Secondly is that the computer crimes have no boundaries or limitations. We can say that cybercrime is any illegal activity that is executed using a computer (especially the internet).

Cybercrime said to be recorded in the year 1820. Abacus, an earliest form of computer has been used in India, Japan, and China since 3500 B.C itself. Charles Babbage who lived during 26 December 1791 – 18 October 1871 was an English mathematician, philosopher, a mechanical engineer, invented the concept of modern digital programmable computer. Because of it, Charles Babbage is also considered as "the father of computers". Today everything from home Air Conditioner to Nuclear Power plant is being run on computers.

3. CYBERSECURITY INITIATIONS

Indian citizens have been victims of numerous instances of data breaches and privacy violations. Safe harbor principles that safeguard the intermediaries from legal action for data breaches. Lack of privacy laws in India allows cybercriminals to misuse users' data on social networks. A safe harbour is an international legal provision safeguarding the performer to reduce or eliminate the liability of the performed in certain situations as long as certain conditions are met. [8]

ICERT, the Computer Emergency Response Team of India [9]- a cybersecurity initiation functioning under the Communications and Information technology ministry of India. ICERT is the national nodal agency for responding to computer security incidents as and when they occur. has revealed that cybercrime incidents are dramatically increasing day by day. As per the Business Standard [10] online news portal, over 2.9 lakh cybersecurity incidents related to digital banking were reported in 2020, Parliament was informed. The Indian Computer Emergency Response Team (ICERT) has reported, a total number of 1,59,761; 2,46,514 and 2,90,445 cybersecurity incidents on digital banking were reported during 2018, 2019 and 2020, respectively, Minister of State for Electronics and IT Sanjay Dhotre said in a written reply to the Rajya Sabha. He further added these incidents included phishing attacks, network scanning and probing, viruses, and website hacking.

Other regulations and notifications issued by regulators such as the Reserve Bank of India (RBI), Department of Telecommunication (DOT), Securities Exchange Board of India (SEBI), the Insurance Regulatory and Development Authority of India (IRDAI), and Computer Emergency Response Team of India (ICERT) mandate cybersecurity standards for their regulated entities, such as banks, insurance companies, telecoms service providers and listed entities.

India has entered various bilateral agreements like a cyber agreement with Russia and a framework agreement with the US. The Indian prime minister's visit to Israel to sign the Indo-Israel cyber framework is yet another initiation of India to regulate its cyberspace. However, these bilateral agreements are not adequate as they are limited in scope. India needs a multilateral treaty with harmonized laws. The treaty should help formulate effective legislation and robust investigative techniques to deal with international cooperation for combating cybercrimes globally. India yet to sign the Council of Europe's Budapest Convention on Cybercrime. This is the first international treaty on cybercrimes. The salient feature of the treaty includes to recommend

safeguards for infringements of copyrights, computer-related frauds, network security threats and child pornography issues. This treaty also prescribes a series of powers and procedures such as the search of computer networks and interception.

4. IMPACT OF INFORMATION TECHNOLOGY ACT

Information Technology Act (IT Act) prescribes penalties ranging from fines to imprisonment for various cyber activities, including hacking, tampering of computer source code, denial-of-service attacks (A denial-of-service (DoS) attack is a type of cyber-attack. A malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning).[11] phishing, malware attacks, identity fraud, electronic theft, cyberterrorism, privacy violations. However, there are no separate set of rules or regulations that regulate the provision of cloud computing services in India.

Further, there is no specific requirement under the IT Act to inform the data subject of a cybersecurity incident. No particular recordkeeping requirements have been prescribed for cyber threats or attacks. In addition, no specific private remedy available for cybercrime victims.

Legal experts say that the IT Act, 2000 is not comprehensive enough and does not even define the term 'cybercrime.' The Indian Penal Code does not use the word 'cybercrime' and also in the amended Information Technology (Amendment) Act 2008. New Information Technology (Amendment) Act, 2008 was passed to address left out provisions in the IT Act, 2000. The new act empowers the Indian government to intercept, monitor, and decrypt computer systems, resources, and communication devices and gave birth to Computer Emergency Response Team-India (CERT-In). However, the new act still lacks to address legal provisions for crime against children and women and data privacy requirements. There is no provision in either the first act or its 2008 amendment that explicitly addresses the capture in electronic sort of violent acts. Further, many cybercrimes related to new developments in technology like cloud computing, artificial intelligence, the internet of things, geotargeting, blockchain, bitcoins, drones, and automation are yet to be covered by the act.

In a historical judgment in Shreya Singhal vs. Union of India, the Supreme Court of India has repealed Section 66A of the Information Technology Act, 2000 as it is violative of Article 19(1)(a) of Indian Constitution. *Shreya Singhal v. Union of India* judgment was pronounced by a two-judge bench of the Supreme Court of India in 2015 on online speech and intermediary liability in India. The Supreme Court struck down Section 66A of the Information Technology Act, 2000. [12]. Repealing the section that offered complainants a specific provision to complain about cyber harassment, bullying, and stalking is no more available for the victims. But, developed countries like the USA and UK are strengthening their fight against cybercrime (Cybercrime is a criminal activity that either targets or uses a computer, a computer network, or a networked device). [13] and they are providing stringent punishment for sending offensive messages through communication service. Of course, in India, the enforcement agencies have the option of booking offenders under the Indian Penal Code like Sections 499 (criminal defamation), 506 (criminal intimidation), 292A (Printing of grossly indecent material), 507 (Intimidation by an anonymous communication) and 509 (word, gesture or act intended to insult the modesty of a woman). However, provisions under a specialized law like the IT Act are an essential requirement instead of the more generic Indian Penal Code, which is often used to deal with physical crimes.

The Indian cyber law ecosystem consists of a series of Indian Acts, including the Information Technology Act 2000 and as amended in 2008, the Indian Penal Code as amended by the Information Technology Act introduced penal sections for cybercrimes and the Indian Evidence Act (as amended by the Information Technology Act) that permits digital evidence before the court of law. The sections of the Bankers' Book Evidence Act (as amended by the Information Technology Act) are relevant to bank records. Same time the Reserve Bank of India Act was also amended by the Information Technology Act. The Investigation and adjudication of cybercrimes follow the Code of Criminal Procedure, Civil Procedure Code, and the Information Technology Act.

However, India does not have any express legislation governing data protection or privacy. Data protection refers to the laws, policies, and procedures that aim to minimize the invasion of other's privacy caused by the unauthorized collection, storage, and dissemination of personal data.

5. DEFENSIVE PRACTICES

India, as a nation, must cope up with an urgent need to regulate and punish those committing cybercrimes, but with no specific provisions to do so. India needs dedicated legislation on cybercrime that can supplement the Indian Penal Code. Legal experts believe that the legislators' primary intention has been to provide a law to regulate e-commerce. With that aim, the act was passed, which is also one reason for its inadequacy to deal with cybercrime cases. Cyber Torts like cyberstalking (Cyberstalking is defined as online following that involves the use of a computer and internet or other electronic means to harass, intimidate or frighten a person or group) [14], cyber obscenity Basically, 'obscenity' means a sexual act or language which shocks people or offends them. When obscenity is committed via the internet, it is termed "cyber obscenity.") [15], cyberdefamation (The tort of cyber defamation is an act of intentionally insulting, defaming, or offending another individual or a party through a virtual medium. It can be both written and oral) [16] and cyberbullying (Cyberbullying is a process of frightening the victim using digital technologies on social media and messaging platforms, gaming platforms, and mobile phones. It is repeated behaviour, aimed at scaring, angering, or shaming those targeted) [17] and harassment.

Cybersecurity expert Vijay Mukhi says, "There's no easy legal recourse available to Indian users, as Facebook data is hosted outside India. If any user must file a complaint against Facebook, the confusion is whether the laws applied would be US cyber laws or Indian ones." He says though cybercriminals (often based outside the country) hack email accounts, websites and impose bogus profiles of celebrities across the web, there is no straight legal route to book them. "The most you can do is track the

machine that originated the hack attack or spam. It is difficult to identify the person behind the crime since cybercriminals use hacked PCs and stolen IP addresses and user data to perpetrate attacks," he adds.[18]

'Provisions to combat cyber frauds have now been introduced under the ITA 2008. However, some issues regarding protection against banking frauds such as phishing, money transfers through online hacking, email frauds, and cybersquatting (including through wilfully misleading domain names), to name a few, have not been addressed separately in the ITA, 2008, even though these are significantly increasing problems.[19]

One way of prevention shall be to deter cybercriminals from attempting the crimes through legal means with stiff punishments. Whether it is a conventional crime using computers or a cybercrime committed over networks, the law enforcement agencies must have adequate knowledge to investigate, standard operational procedures, and stringent rules to bring them before the court of law. In addition, stringent and more specific laws and regulations should be developed and implemented to punish the cybercriminals to avoid recurrence of such criminal breaches.

6. CONCLUSION

At this juncture, we can conclude that, India needs the following cybercrime defensive strategies to combat cybercriminals and secure India from cyber-attacks:

- Active cyber defense technologies and processes should be implemented to support central and state government agencies and organizations.
- Stringent rules and regulations should be developed and applied to bring the errands before the court of law.
- Law enforcement agencies should be imparted with adequate knowledge and standard operational procedures to investigate cybercrimes.
- Overlapping of regulatory bodies should be avoided, and a cybersecurity authority should deal with cyber issues.
- Cybersecurity education should be part of a regular stream of education, and awareness should be created at the school level.
- India should be part of international treaties on cybersecurity programs and implement the agreed-upon defensive strategies.
- Last but not least, awareness should be created among public to come forward and register a case in the nearby police station if anyone falls prey to cyber-attacks.

7. REFERENCES

[1] Refer: https://www.thehindu.com/news/cities/mumbai/cyber-sabotage-led-to-october-2020-outage-in-mumbai-minister/article33964939.ece
[2] Refer: https://en.wikipedia.org/wiki/Cyber_spying#
[3] Refer: http://download.microsoft.com/download/
[4] Refer: https://www.imperva.com/learn/application-security/website-defacement-attack/
[5] Refer: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html
[6] Refer: http://www.legalserviceindia.com/legal/article-836-cyber-law-in-india-it-act-2000.html
[7] Refer https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html.
[8] Refer: https://www.investopedia.com/terms/s/safeharbor.asp
[9] Refer: https://www.cert-in.org.in/
[10] Refer: https://www.business-standard.com/article/finance/over-290-000-cyber-security-incidents-related-to-banking-reported-in-2020-121020401220_1.html
[11] Refer: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
[12] Refer https://en.wikipedia.org/wiki/Shreya_Singhal_v._Union_of_India.
[13] Refer https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime.
[14] Refer: https://us.norton.com/internetsecurity-how-to-how-to-protect-yourself-from-cyberstalkers.html
[15] Refer: https://digiinfomedia.online/cyber-obscenity/
[16] Refer: https://www.latestlaws.com/articles/cyber-defamation-the-court-of-social-media/
[17] Refer: https://www.unicef.org/end-violence/how-to-stop-cyberbullying
[18] Refer https://www.business-standard.com/article/technology/cyber-laws-loopholes-aplenty-111111800098_1.html.
[19] Refer Page #25 @ https://media.neliti.com/media/publications/28731-EN-cyber-crime-law-in-india-has-law-kept-pace-with-emerging-trends-an-empirical-stu.pdf.

