ILE WEEKLY REVIEW

VOLUME I AND ISSUE V OF 2023

APIS – 3920 – 0037 | ISBN - 978-81-964391-3-2

Published by

Institute of Legal Education

https://iledu.in

AN OVERVIEW OF CYBERCRIME THREATS IN INDIA: A BREACH OF PRIVACY

AUTHOR - GARIMA PRADHAN, STUDENT AT ST. XAVIER'S UNIVERSITY, KOLKATA

BEST CITATION - GARIMA PRADHAN, AN OVERVIEW OF CYBERCRIME THREATS IN INDIA: A BREACH OF PRIVACY, *ILE WEEKLY REVIEW (ILE WR)*, 1 (5) OF 2023, PG. 1-5, APIS – 3920 – 0037 | ISBN - 978-81-964391-3-2.

ABSTRACT

Cybercrime is an emerging global issue. It is a result of highly networked information systems and highly evolved technologies. Tremendous rise in cybersecurity reports has been seen, with more than 100 cases filed every day compared to the year 2018. The criminals have the liberty of operating from home and the advancement in AI have given unauthorized access to confidential information effortlessly. Some of the recent cyber-attacks in 2023 comprises of DDoS attacks, hacking, carding, AI scams, social engineering, phishing, ransomware attacks, cloud third party threats, mobile malware, and the list goes on. This paper includes a detailed discussion of cybercrimes cases in the cyberspace with an Indian perspective. The data connected to such crimes in India from 2019 to 2023 are also analysed in this article and further recapitulated the legislation enacted to combat cybercrime.

KEYWORDS: Cybercrime, Cybersecurity, Breach, IT Act, Government of India

I. INTRODUCTION:

The evolution of technologies, rapid proliferation of internet access and the emergence of digitalization in India have set the ground for a surge in digital crime. From primary school students to governmental agencies, internet access has become a basic necessity for all. Despite attempts of legislatures in policy building, particularly in introducing several laws under the IT Act, there are many areas left untouched like a separate statute for online transactions and IPR concerns in India or any adequate legal sanctions.

Cyber threats include social engineering attacks, cyber terrorism, cyber warfare, Wanna cry malware attack, Not Petya, Crypto jacking, Mage cart attack, BEC, impersonation, carding, other ransomware attacks and so on. In 2000, the first cybercrime was reported in India[1].

According to NCRB, number of registered cybercrimes in India jumped to 50,035 cases in 2020 compared to in 2019 with 44,735 cases[2] and now more than 100 cases are reported every day resulting data breaches, cyber harassment, child exploitation, online scams and many more.

In third quarter of 2022, there was 28% increase in cybercrimes, globally, compared to the same period in the previous year. Again, in response to the Russian-Ukrainian war in 2022, an increase by 38% in 2022 was observed compared to 2021[3].

To combat the growing numbers, Government of India in cooperation with different individuals and organizations are working towards variety of approaches which includes India's most recent, popular and supported digital projects

[1] C. MOUNTAIN VIEW, "Symantec Announces MessageLabs Intelligence 2010 Annual Security Report."

[2] NCRB- Report of 2020 https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.1.pdf

[3] *Cyber Security Report of 2023- CHECK POINT*

ILE WEEKLY REVIEW

VOLUME I AND ISSUE V OF 2023

APIS – 3920 – 0037 | ISBN - 978-81-964391-3-2

Published by

Institute of Legal Education

https://iledu.in

initiated by the current political party BJP (Bhartiya Janata Party) is the UIDAI (Unique Identification Authority of India) project. Under this the government provides biometric IDs for all the citizens of India that contains their personal information for its record. The biometric ID also known as Aadhaar which has 12-digit number, generated by collecting 10 fingerprints, iris scans, birthdate and address and are linked with all other government IDs such as PAN card, Voter card and financial accounts making it susceptible to data breaches, posing high risk of security and privacy of information. Recently government has introduced a 'replica' of the Aadhaar known as Masked Aadhaar (m-Aadhaar) keeping in mind the rise in cyber-attacks in India accompanied by massive growth of e-commerce. In the masked Aadhaar out of 12-digits only 4-digits are visible, instead, it provides the residents a virtual ID (VID) which works equivalent to the original Aadhaar number acting as a double security or two-way authentication factor. In addition, preventive measures on how one can defend themselves on a personal basis will be further discussed in this paper.

II. COMMON TYPES OF CYBER CRIMES

Wide range of illegal activities are committed through different modes and multiple ways in the cyberspace using computers, internet or networks. The most prevalent attacks are: -

a. Ransomware attacks- are a specific type of malware attacks where the malicious software encrypts a set of user's information making or rendering it inaccessible until a ransom amount is paid to the criminal within a specified timeframe.
   Malware Attack- Malware is a malicious software designed to compromise the devices, network and gain unauthorised access to the system without knowledge to the user with an intention to extract sensitive information.

b. Phishing- it is one of the most common and popular type of social engineering attacks which is a method where individuals are deceived and tricked to reveal their personal and sensitive information such as financial details etc. This act is usually practised electronically and some common phishing techniques used by the criminals are Email phishing, BEC (Business Email Compromise), Tax Refund Scams, Google Drive phishing, Payment Phishing, Spear Phishing, Vishing, Man-in-the-Middle (MitM) Phishing.
   Apart from this, at an individual level, when a person lands up on fraudulent websites or email spooking by attackers, luring users to download malware or provide direct access to their systems thereby extracting all of the information of the user.

c. SIM-swapping- it is also called SIM card swap or SIM hijacking where the attacker targets the victim's phone number linked with banks accounts and other valuable accounts. Thereafter, pretexting to convince the authenticity to the users and fraudulently transferring the victim's phone number to the criminal's SIM card. This way the attacker gets access to all online accounts, receive OTPs conducting monetary transactions etc.

d. IoT (internet of things) Hacking- IoT devices such as smart devices, industrial sensors, medical devices etc, embedded with internet connection are vulnerable to hacking or unauthorised access or control over the device by a hacker.
   Subsequently leading to privacy breaches, DDoS attacks, safety risk and many more.

e. State-sponsored cyber warfare or Cyber Espionage- it is an attack conducted by government or the state against other governments, organizations or individuals. In consequence, damaging

ILE WEEKLY REVIEW
VOLUME I AND ISSUE V OF 2023
APIS – 3920 – 0037 | ISBN - 978-81-964391-3-2
Published by
Institute of Legal Education
https://iledu.in

the economic, political, national security, other collateral damage and erode public confidence of that country.

f. DDoS (Distributed Denial-of-Service)- this method is used to flood the user's device with so much malicious or illegitimate traffic and make it difficult to operate any further. The devices are first infected with malware which creates a gateway for the criminal to control the system. This attack can result to huge financial losses and sometimes even damages the user's reputation.
g. Zero-day attack- the criminal discovers the vulnerabilities also known as zero-day exploits, in the software or the operating system that is not known to the vendor or developers and then stealing confidential data from the user. These zero-day exploits are of high value sold to organizations or governments who would further use such exploits or vulnerabilities for criminal purposes.
h. Identity theft- it is an act where the criminal steals the victim's identity or information and indulge in illicit activities in their name.

III. CYBER LAWS: IPC, SLL & INFORMATION TECHNOLOGY ACT,2000

Reported crimes in India have been listed into mainly three categories

a. IT Act cases,
b. IPC (involving computer as medium/target) cases, and
c. Special Acts & Local Laws (SLL) (involving computer as medium/target) cases.

A. IT (Information Technology) Act, 2000---
This act was passed when the cybercrime cases were on rise in the nation. It legalized e-commerce activities and other acts such as IPC, Evidence Act, RBI Act were amended to align with the Act of 2000. In order to address emerging issues such as child pornography accelerating child exploitation, IT act of 2000, was revised in 2008. The 2008 amendment also created National Critical Information Infrastructure Protection Centre (NCIIPC) and designated as National Nodal Agency to secure the confidential information about the Nation. Despite the implementation of the Act, it was still found to be inadequate in several ways. The haste with which the Act was passed by the Parliament is viewed the cause for its insufficiency.

B. IPC cases---
The cases under IPC grew exponentially in 2019 by 58% in comparison to 2018. This was the result of digitalization. There have been several reports of new fraud instances, and the IT Act of 2000 is falling behind. IT act read with IPC was found effective in reducing these to some extent.

Government continues to encounter difficulties in setting up separate legal court system and enforcement procedures for cyber threat cases.

IV. STATISTICS & ANALYSIS OF CYBERCRIME IN INDIA (2019-2023)

National Cyber security Coordinator Lt. General Rajesh Pant in one of his interviews stated that there had been more than 1.25 lakh crore loss in the cyber world in 2019, and the rise will continue with the advent of 5G networks and other tech spread.

Cybercrime had jumped up to four times in the four years, according to NCRB statistics from 'Crime in India 2020'. In the report[4], there were total 29643 cases registered under the IT Act, the majority of which were computer-related (leading state UP with 3803 cases), identity theft (first Bengaluru with 3513 cases), Personification-based cheating (Bengaluru-6486 cases), Publication of obscene acts in electronic form-- 6216 cases. Total offenses under IPC (Involving Communication Devises as Medium/Target) and SLL (Involving Communication Devises as Medium/Target) were 20201 and 191 respectively. To this regard the National Cyber Security Strategy of 2020

[4] https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE%209A.2.pdf

was conceptualized to ensure a safe a secure cyberspace for the nation and its people.

The report also indicated fraud as a primary aim in 60.8% of the cybercrime in 2021 accompanied by sexual exploitation with 8.6% and extortion with 5.4%.

India by 2022 was the top five targets in the Asia Pacific (APAC) region for attacks on cyber security[5].

Digital transactions are at its peak, from buying groceries to transferring huge amount between banks both nationally or internationally. As per the Press Information Bureau in Delhi, online payment space in India has increased from 20.71 billion to 55.54 billion in the first quarter of 2023.

Overall cyber-attacks in India increased by 18% in Q1 2023[6] compared to the same time in 2022, owing to developments in AI tools such as ChatGPT. This tool supports real-time interactions, and hackers can easily generate sophisticated codes or programmes in a short duration, effortlessly. Education and research sector had extensive increase in the number of attacks globally with 2,507 cases weekly per entity amounting to 15% increase compared to first quarter of 2022, reported by Check Point in 2023.

V. CONCLUSION

The consequences of the growing cyber security, concern among individuals, government agencies or organizations are majorly due to low level of human development, shortage of IT security products and other resources. The Government of India declared in 2012 that it would grant financing to Indian enterprises to buy foreign firms with advanced and innovative cyber security technology[7]. Moreover, IT security auditors are also needed to validate the effectiveness of the programmes and controls for management.

It is impossible to eliminated the crimes in cyber space completely, instead it can be put to its limit by way of introducing a stronger law or policy. But it should be kept in mind that even in the global history, such initiative has not given us the desired results. The crimes in the cyberspace continued to increase at a tremendous rate every year. Moreover, women and children are likely to be an easy target of such crimes who are usually considered the weaker sections of the society which is the result of lack of awareness. Studies show that many cases are left unreported which is also due to lack of awareness about the laws pertaining to these crimes. At the same time the government have other national issues to handle like unemployment, poverty and other post covid-19 affects, thus being unable to give cybersecurity its current priority. The frequency of these cases is often disregarded allowing oneself to be vulnerable. A combination of proactive network security measures, skilled cybersecurity professionals and user awareness of their right and duties can significantly reduce the impact of these issues.

VI. REFERENCE

a. C. MOUNTAIN VIEW, "Symantec Announces MessageLabs Intelligence 2010 Annual Security Report."
b. NCRB report of 2018-2020 on cybercrime
c. Cyber Security Report of 2023- CHECK POINT
d. the Cyberthreats to Financial Organisations report of 2022
e. NCRB report (2020), cybercrime related to IT Offences, IPC cases, SLL cases.
f. Editorial team- India sees sharp increase in cyberattacks in Q1 2023. Retrieved from https://economictimes.indiatimes.com/tech/technology/sharp-increase-in-cyberattacks-in-india-in-q1-2023-report/articleshow/100096450.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[5] According to the Cyberthreats to Financial Organisations in 2022 report

[6] Economic Times- India sees sharp increase in cyberattacks in Q1 2023; https://economictimes.indiatimes.com/tech/technology/sharp-increase-in-cyberattacks-in-india-in-q1-2023-report/articleshow/100096450.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

[7] https://www.thehindubusinessline.com/info-tech/Govt-will-help-fund-buys-of-foreign-firms-with-high-end-cyber-security-tech/article20416307.ece

g. Thomas K. Thomas (2012) - 'Govt will help fund buys of foreign firms with high-end cyber security tech'. Retrieved from https://www.thehindubusinessline.com/info-tech/Govt-will-help-fund-buys-of-foreign-firms-with-high-end-cyber-security-tech/article20416307.ece