Page 1953 - 1962 **DOI:** *https://doij.org/10.10000/IJLMH.118458*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 5

2024

From Bytes to Battles: India's Struggle Against the Surge of Cybercrime

JASMINE SHARMA[1] AND ABHISHEK CHATTERJEE[2]

ABSTRACT

India is moving towards the digital era with its flagship campaign "Digital India" and it brings innumerable opportunities in terms of innovation and networking. Nonetheless, the advancement of technology that has developed quite rapidly over the years, has also brought increased cases of cybersecurity threats which are dangerous to any individual, firm or critical structures. This article looks at the relationship between India's digital evolution and the rise of cyber threats, as a study shows cybercriminal attacks rising 63.5% between 2017 and 2018, as reported by the NCRB. Thus, pointing out the most typical kinds of cybercrime, including advanced hacking, identity theft, and ransomware and phishing attacks, the article underscores the urgent issues that hamper the response. This is a problem for India because the laws are outdated and the police force and other law enforcement agencies generally lack technical know-how. This article provides a set of practical recommendations based on the recent data, including the considerable financial losses in the banking sector as a result of cyber events. Among them are enhancing cybersecurity having the best technologies, increasing people's awareness, publishing, and promoting collaboration between both governmental and non-governmental organizations as well as carrying out amendments to legal regulation concerning cybersecurity. In conclusion, it can be noted that the article has the imperative call for going forward and taking active battles against cyber criminalities and that no nation through passivity and complacency in the world today can ensure its future safety despite its nascent technological rights lest it turns the threats of cybercriminalities to the opportunities for future growth.

***Keywords**: Cybersecurity Threats, Cybercrime, Identity Theft, Digital Transformation, Digital India.*

I. INTRODUCTION

Technological advances in the contemporary society have led to the growth of new forms of social relations based on the access of information. In India the ongoing Digital India scheme of the Government also aims to leverage this power for optimizing government services, enabling e-commerce, and encouraging storage of important data in cloud infrastructures. But

[1] Author is an Advocate at Delhi District Courts, India.
[2] Author is an Advocate at West Bengal High Court and District Courts, India.

 [ISSN 2581-5369]

the advancement of the digital and information technologies has made the country more susceptible to cybercrimes. Such criminal activities, including hacking and identity theft, ransomware, phishing attack, and the like are among the dangerous forms of the threat that people, organizations, and the country at large are facing. India has been on the path to becoming a digital economy, and with the change, comes benefits and pitfalls. The availability of internet services has promoted the financial advancement and social development processes, but it has enhanced episodes of cybercrimes. According to the NCRB, the occurrence of cybercrime increased by 63.5 per cent between the years 2017 and 2018. As the country continues to expand its presence on the world wide web, it becomes an even more appealing entity to cyber criminals both local and foreign.

The legal and institutional frameworks designed to combat these crimes, such as the Information Technology Act, 2000, and the National Cyber Security Policy, 2013, have been instrumental in addressing some of these challenges, but they are not enough to fully counter the scale and complexity of modern cyber threats.[3]

II. THE DIGITAL INDIA INITIATIVE: A DOUBLE-EDGED SWORD

Digital India is one of the massive initiatives undertaken by the center that aims at developing India into a digitally enabled nation. It was started in 2015 to deliver government services electronically, minimize paper work and increase accountability. At the same time, the use of the Internet is encouraged, in particular, cloud solutions that enable both the government and private enterprises to store and process extensive data on their servers. Although these goals can be considered as good and desirable, they pose heightened security threats.

Cybercrime, by its very nature, thrives in environments where sensitive data is stored and transferred online. The more India integrates digital technologies into its economy, governance, and daily life, the more susceptible it becomes to various forms of cyberattacks.[4] The internet's ubiquity has made it possible for malicious actors to target not just large corporations and government entities, but also individuals who may not be fully aware of the risks involved in online activities. Furthermore, many Indian citizens lack adequate knowledge about cybersecurity practices, making them easy targets for phishing scams, identity theft, and other forms of online fraud.[5]

[3] Id. at 313.
[4] Id.
[5] Bahuguna, supra note 3, at 313.

 [ISSN 2581-5369]

(A) Categories of Cybercrime in India

Cybercrimes in India can be broadly classified into the following categories:

1. Hacking and Unauthorized Access: Computer hackers, which is a situation where a person accesses another's computer without permission, is on the increase in India. These incidents can lead to data leakage, that is information being stolen or becoming unusable. Most hacking incidents in India are for monetary reasons, but some of them have political or even ideological backgrounds.[6]

2. Identity Theft: The most reported type of cybercrime in India is identity theft. In cybercrimes, hackers offer to grab Identity numbers, Aadhaar numbers, bank account details, or credit card information intending to take part in scams. The financial sector has suffered so much from such crimes in a way that many people and institutions lose lots of money.[7]

3. Phishing and Ransomware: These days phishing attacks, which involve sending fake emails and messages to people in order to get them to reveal personal information, have become highly developed. Ransomware attacks, where hackers lock up data and demand payment for its return, are also an emerging problem for Indian organisations.[8]

4. Cyberstalking and Cyberbullying: They noted that the rates of cyberstalking and cyber bullying are on the rise also correspondent to the rise in the use of social media platforms. These are heinous crimes which have severe psychological effects on the victims especial females and children, and very often they remain unknown to police due to threats or stigmatization.[9]

5. Financial Fraud and Cryptocurrency Crime: The rise of digital payments and cryptocurrency usage has opened new avenues for financial fraud. Cybercriminals exploit vulnerabilities in online banking systems or create elaborate schemes to defraud individuals and companies of large sums of money. The growing anonymity provided by cryptocurrencies has also facilitated the rise of money laundering and other financial crimes.[10]

(B) Challenges in Addressing Cybercrime

The acute problem of fighting cybercriminals in India is the general low level of cybersecurity development in the country. Unfortunately, the Information Technology Act, 2000 and the National Cyber Security Policy, 2013 do not suffice because technology is not static hence; the

[6] Id.
[7] Id. at 314.
[8] Jack Nicholls et al., "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape", 9 IEEE Access 163965, 163967 (2021).
[9] Bahuguna, supra note 3, at 314
[10] Nicholls, supra note 11, at 163968.

 [ISSN 2581-5369]

threats that individuals face are dynamic.[11] Police organizations themselves usually do not possess the required technical knowledge and equipment that will help them catch and bring cybercriminals to justice. Most of the officers lack adequate training in collection of digital evidence and hence the required evidence to make convictions is hard to come by.

Additionally, these criminal are international in most cases and this makes jurisdiction a major challenge in the prosecution of these crimes. Cybercrime is a global issue and demands some kind of cooperation at the international level; however, the mutual legal assistance treaties and similar treaties and agreements are insufficient to deal with the problems of digital crime.[12]

The fact that conviction rates of cybercrime in India remains extremely low only aggravates the situation. For instance, Maharashtra, which comes under the top list of states for cybercrime rates in India reported 10,000 plus cybercrime cases from 2012 to 2017.[13] However, during this time 34 convictions were won, leading to a conviction rate of only 0.3%. This is so because while many people may report cases of cybercrime to the police, the number of people who are actually prosecuted and convicted is very low.

III. DATA ANALYSIS AND TREND

(A) The Emerging Risk of Cyber Hit in Indian Banking Industry

India banking sector has undergone a drastic change with the introduction of digital financial services in the last decade especially internet banking, mobile banking and real time payments. Though these innovations have increased convenience and access for millions of customers it has brought new risks at the same time. The sector has unfortunately become more appealing to cybercriminals, who now look for weaknesses in the implemented security, and use phishing, identity theft, ATM fraud, and hacking as some of the most frequent techniques. Modern computer crimes not only affect every user, but also reduce public trust in online banking, which poses a potential threat to the entire financial system.

(B) Increasing Volume of Cybercrime

In 2016, India saw a marked increase in the volume of cybercrime incidents, particularly in the banking and financial sector. The National Crime Records Bureau (NCRB) recorded 16,468 cases of cybercrime related to banking between 2014 and 2016, representing an alarming trend.[14] The rise in cybercrime has coincided with the rapid expansion of online banking, mobile

[11] Bahuguna, supra note 3, at 315
[12] Iqbal & Beigh, supra note 6, at 188.
[13] Bahuguna, supra note 3, at 316.
[14] National Crime Records Bureau (NCRB), Cyber Crime Statistics 2014-2016, Ministry of Home Affairs, Government of India, 2017. Available at: [NCRB Cyber Crime

 [ISSN 2581-5369]

payments, and digital wallets, which have grown exponentially over the same period.

The following table presents data on the domain-wise breakdown of cybercrime incidents in India.

Table 1: Domain-wise Cybercrime Incidents in India (2014-2016)

Domain	No. of Cases Registered
Banking System	16,468
Social Media	328
Email Hacking	125
Lottery Fraud	42
Job Fraud	49

Source: National Crime Records Bureau (NCRB), "Cyber Crime Statistics 2014-2016," Ministry of Home Affairs, Government of India, 2017.[15]

The overwhelming majority of cybercrime cases involve the banking system, with 16,468 incidents compared to far fewer cases in social media, email hacking, and other domains. This underscores the banking system's susceptibility to cyberattacks and highlights the pressing need for improved security infrastructure.

(C) Financial Losses Due to Cybercrime

The financial impact of cybercrime has grown at an alarming rate, as evidenced by the year-on-year increases in both the number of cases and the value of losses. From 2015 to 2018, financial losses due to cybercrime rose dramatically. This growth is highlighted in Table 2, which tracks cybercrime cases and financial losses over a three-year period.

Table 2: Financial Losses Due to Cybercrime (2015-2018)

Year	No. of Cybercrime Cases	Financial Loss (in Rs. crore)
2015-16	1,191	42.3
2016-17	1,372	109.6

Statistics](https://ncrb.gov.in/sites/default/files/Cyber%20Crime%20Statistics.pdf) .

[15] Reserve Bank of India, Annual Report on Digital Payments, 2018. Available at: [RBI Digital Payments Report](https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=243#ch2) .

 [ISSN 2581-5369]

2017-18	2,059	210.3

Source: Reserve Bank of India, "Annual Report on Digital Payments," 2018.[16]

It has been analysed that between 2015-16 and 2017-18, cybercrime cases increased from 1,191 to 2,059, representing a nearly 73% rise in reported incidents. More significantly, the financial losses grew almost fivefold, from Rs. 42.3 crore to Rs. 210.3 crore. This sharp increase in financial losses signals not just a higher frequency of cybercrimes but also more significant and sophisticated attacks that result in greater monetary damages. This data reflects an escalation in the scope of cybercrime, with criminals employing increasingly complex methods to defraud individuals and institutions.

IV. UNDERSTANDING THE ISSUE THROUGH DATA

Information on cybercrime in the Indian banking system shows the increased threats from 2014 to 2016, 16,468 times, which testifies to the systematic problem of financial organizations. This rising incidence is parallel to a sharp rise in the extent of financial loss where the amount has soared from Rs. 42.3 crore in 2015-16 to Rs. 210.3 crore in 2017-18. The fact that losses have been significantly on the rise coinciding an equivalent rise in the number of cybercrime cases, show how well orchestrated the criminals are, and the increased importance for enhanced security and active defense in the banking sector.

The implications of these findings are especially important for developing appropriate measures. First of all, it is necessary to educate consumers since many thieves rely on the client's lack of knowledge concerning secure banking. Due to the high speed of threats development in cyberspace, the movement from the post-performing to the pre-performing model is crucial for banks to be prepared for the attacks and prevent vulnerabilities. Risk management can also be boosted by exaggerating the consumer awareness programs and endorsing the best practices; on the other hand, continuous training of the employees will improve the institutions' resilience.

To remain well-equipped to counter the emergent threat of cybercrime in the coming year and beyond, there is no option for financial institutions to adopt the latest technologies such as the Big Data Security Analytics to get real-time transaction monitoring, and the ability to detect any abnormalities. Besides, encouraging the cooperation of banking institutions in sharing

[16] Goel, Seema, Cyber-Crime: A Growing Threat to Indian Banking Sector, 5(2) Indian Journal of Banking 552, 553 (2016). Available at: [Indian Journal of Banking](https://www.researchgate.net/publication/316364364_Cyber-Crime_A_Growing_Threat_to_Indian_Banking_Sector) .

information on new risks can also improve general security. This effort should also be complemented with the government effort of enhancing the legal instruments for cyberspace. These measures should be adopted hand in hand with creating the public awareness regarding secure banking and arising risks regarding cybercriminal activities which endangered the Indian banking sector, thus, rebuilding the confidence of the population in the safe online payments.

V. SUGGESTIONS: NAVIGATING THE CYBERCRIME LANDSCAPE

In wake of this newly felt technological advancement in India, one of the challenges that have cropped up is that of cybercrime. To effectively combat this rising tide of online threats, here are some practical suggestions:

1. Enhancing the Framework of Cybersecurity

In order to improve their capacity to protect against cyber threats, financial institutions and businesses must increase the level of spending on cybersecurity measures. For instance, there is Big Data Security Analytics (BDSA) that can be quite effective at that. With help of machine learning and all kinds of monitoring tools, it is possible to detect suspicious actions and possible breaches prior to the development of real catastrophes. The State Bank of India has adopted intelligent systems to detect frauds and these systems nurture a way to analyze transactions to flag such activities. Also there is need to assure usage of stricter encryption methods like that of an AES and even multilayered …authentication measures to cut down on a chances of an in unauthorized personnel getting access to sensitive data. The functionalities like, data protection and securing of sensitive information, are governed by regulation such as the Information Technology Act, 2000[17], therefore the need to conform to standards made available.

2. Awareness and Education of the Public

Educating the public is important in the fight against cybercrime since people will be able to stand on their own. For instance, the Indian government has introduced the Cyber Awareness Program that is to help citizens identify the main threats of phishing scams and practice safe behavior on the Internet, as well as learn the reasons for personal data protection .Educational campaigns enforced by the Indian Computer Emergency Response Team (CERT-In) are composed of the raising of the average user's awareness about typical cyber threats and how to prevent them. Program launched by the Indian government aims to educate citizens on recognizing phishing scams, practicing safe online behaviour, and understanding the importance of protecting their personal information. Awareness campaigns led by the Indian

[17] Information Technology Act, No. 21 of 2000, India.

 [ISSN 2581-5369]

Computer Emergency Response Team (CERT-In)[18] focus on helping users understand common cyber threats and how to avoid them.

Financial institutions should also come in to supplement their customers, providing them with adequate ways that can help in sensitization. For instance, HDFC Bank offers periodic training sessions and lectures on cybersecurity measures for the clients who offer useful information that enables users to protect themselves from cyber criminals. Moreover, conveying cybersecurity in schools through programs that state governments have developed including the Cyber Safety Program will help the younger generation prepare for a digital security environment.

3. Interface between stakeholders

Cybercrime is difficult to combat if not fought with a team approach. This is because banks, governmental departments, and law enforcement agencies should work in synergy. Unification of a primary source of information that is shared concerning the threats experienced will improve response to the threats hence the need to adopt it. I4C or Indian Cyber Crime Coordination Centre[19] was established and meant to improve cooperation between the stakeholders, to share the intelligence data on cyber threats, and to implement the single operations with the threats. Furthermore, commitment from private sectors could be also very helpful in this regard. The NASSCOM works in liaison with police forces throughout the country to enhance reporting and handling of cybercrimes.

4. Detailed Understanding and Support from the Legislative and the Regulatory Systems

To operate effectively against digital competitiveness, it is necessary to incorporate alteration within legal regulation of cybercrime in India. Actualization of such regulations for instance the Personal Data Protection Bill that seeks to protect personal data and put rigid data protection standards on business can spur compliance and accountability. Specifically, the provisions aimed at strengthening laws enforcement agencies and improving their capacity to investigate and prosecute individuals that committed computer crime will discourage others from committing the offenses in the future and afford victims' justice. For instance, the Cyber Crime Investigation Training Centre named by the government provides an operative training for police staff to address cybercrime-related cases. Also, International Treaties such as Budapest Convention on Cybercrime[20] to which India is a signatory can bolster the legal framework and

[18] Cyber Awareness Program, Government of India, available at [https://www.cyberawareness.gov.in]
[19] Indian Cyber Crime Coordination Centre (I4C), available at [https://www.cybercrime.gov.in]
[20] Budapest Convention on Cybercrime, available at https://www.coe.int/en/web/cybercrime/the-budapest-convention.

 [ISSN 2581-5369]

global collaboration against cyber evils.

5. In the ordinary evaluation, the constant assessment and monitoring processes are part of the program.

Last but not least, as the new threats and challenges emerge in the digital environment we also have to learn how to adapt our defense mechanisms. Programs to review and audit on the level of organizations security management, as well as, considering the outcomes of public awareness activities, will aid organizations in preventing the escalation of threats. Using NIST Cybersecurity Framework is a common strategy through which various organizations are able to address and manage cybersecurity risks. Furthermore, performing penetration test and vulnerabilities assessments can show where an organization lacks protection on a regular basis. Therefore, while evolving strategies India can be able to sustain its fight against the growing menace of cybercrime.

VI. Conclusion

India in general represents a progression in the digital world which raises the problem of the increase in cybercrime that has a powerful and daunting impact on the security of the country, its economy and the trust of its inhabitants. Advanced technology has become a part of society in recent years which formed a positive impact but recently, tech-savvy criminals exploit the chinks. In this article, the good news is that a detailed approach on how to tackle all these pertinent issues has been expounded with the call for positive and complementary actions. In order to prevent different forms of cybercriminal activity, one has to improve the situation with cybersecurity through increasing investments in the sphere, as well as applying the most effective solutions. Mass consciousness and knowledge raising thereby become the important measures for making a person protect himself from a cyber threat. In addition, increased cooperation among professionals, including governmental legislators and law enforcement bodies, and other businesses will help to improve attitudes to counter cyber threats.

It is not only high time to modernize the legal regulations, but it is also a real necessity due to the new forms of digital threats. Increase of laws and improvement of conditions for police work and investigation will create a stable base for fighting with cybercriminals, and, in the same time, protect the rights of victims. This way, institutions will be able to detect fluorescence of new threats, enhancing cybersecurity making the digital environment secure. The journey from bytes to battles underscores a critical reality: preventing information criminal activities is no longer simply a technical issue but a national one as well. So there is a need, now more than ever before, to come together post-independent as a country India in this digital age of the world.

 [ISSN 2581-5369]

Combined, they can contribute to the creation of a more secure environment for innovation, and citizens to prosper in the safe digital environment.

Thus, accepting these important strategic steps, India can use the threat of cybercrime as the potential for development and strengthening. The battle against cybercrime ensues and acting together and with passion, India can turn into a model of safe cyber space in the world of rapidly integrating global networks.

*****

 [ISSN 2581-5369]