# CYBERCRIME AND INDIAN BANKING SECTOR: A CRITICAL ANALYSIS

Marisha Shandilya, Advocate at Patna High Court


## ABSTRACT

The rapid digital transformation of the Indian banking sector has revolutionized customer experience through enhanced accessibility, convenience, and efficiency. However, this technological advancement has also introduced complex cybersecurity challenges. The growing reliance on online transactions, mobile banking, and digital payment systems has made financial institutions prime targets for cybercriminals. The anonymity, global reach, and sophistication of modern cyberattacks especially those driven by artificial intelligence and deepfake technologies have significantly increased the risk of financial fraud and data breaches. Despite the Reserve Bank of India's proactive measures, including the Cyber Security Framework for Banks and adherence to ISO/IEC standards, vulnerabilities persist due to evolving attack methodologies and limited consumer awareness. The Digital Personal Data Protection Act, 2023, further strengthens the legal framework, yet the effectiveness of these measures relies on their consistent enforcement and the active participation of financial institutions. Strengthening cybersecurity architecture through continuous technological upgrades, employee training, AI-driven fraud detection, and public awareness campaigns is essential to safeguard trust and resilience in India's digital banking ecosystem. The study concludes that while digitalization drives economic growth, it also amplifies the risk landscape, necessitating a balanced approach that promotes innovation without compromising security.


**Keywords:** Cybersecurity, Digital Banking, Fraud, RBI Regulations, Artificial Intelligence

# INTRODUCTION

## 1.1 Introduction

Technological progress has resulted in unforeseen outcomes, creating various avenues for criminal activities in both digital and physical realms. Communication tools such as text messaging, email, and social media have streamlined traditional crimes like fraud and stalking, minimizing the likelihood of detection by law enforcement. The combination of advanced computers, high-speed internet, and storage devices has allowed the widespread distribution of illegally replicated software, media, etc on a global scale.[1]

In today's age of technological advancement, the Indian banking sector has undergone significant transformation. This has happened due to the fast application of new technologies like machine learning, artificial intelligence, blockchain, etc. but with this advancement comes the problem of increasing cyber risks. In the initial stage, the developed nations were the primary target of cyberattacks but now the situation has changed and Indian companies have become equally vulnerable. The Computer Emergency Response Team has "reported over 17,000 cyberattacks on Indian banking and finance sector in 2022".[2] The RBI has also informed a parliamentary panel that there has been an increase in ransomware cases on banks and the data stolen from such attacks has been available in the dark web which poses a serious concern[3].

BioCatch's *2025 Digital Banking Fraud Trends in India* report reveals a sharp rise in financial crime, with fraud cases in Indian banks tripling in 2024 compared to the previous year. Alarmingly, nearly 90% of incidents reported to the RBI this fiscal actually occurred earlier, masking the true extent of ongoing fraud. Despite this reporting lag, losses have already jumped by 715% in just the first half of FY 2024–25, reaching about ₹21,367 crore ($2.56 billion). Among these, *digital arrest scams* stand out as the most devastating, causing roughly ₹2,000 crore ($240 million) in losses, often traced to syndicates operating from Myanmar, Cambodia, and Laos. Meanwhile, banks are struggling to curb *mule accounts*—used to channel illicit money—because RBI rules require court approval before freezing or blocking them.

[1] Jitender K Malik, Sanjaya Choudhury, "*A Brief review on Cyber Crime - Growth and Evolution*" https://www.pramanaresearch.org/gallery/prj-p580.pdf, (visited on December 10, 2023)

[2] Akanki Sharma, "*Cyberattacks on Indian Banks and Finance Sector*", https://b2binfomedia.com/cert-reported-over-17000-cyberattacks-on-indian-banking-and-finance-sectorin2022,(visited on October 1, 2023).

[3] Jatin Takkar, "*Banking and finance increase in ransomware cases in banks, Economic Times*", June 05, 2023, https://economictimes.indiatimes.com/industry/banking/finance/banking/increase-in-ransomware-cases-in-banks-rbi-tells-parliamentary-panel/articleshow/100749514.cms?from=mdr, (visited on October 1, 2023).

Altogether, the findings highlight how financial crimes are becoming more sophisticated while regulatory and procedural bottlenecks continue to slow down effective response.[4]

The banking sector has experienced a broadening of its services, aiming to enhance customer convenience through technological advancements. However, the persistent challenge of cybercrime remains. Information available online is highly vulnerable to attacks by cybercriminals. These cybercrimes lead to substantial financial losses, impacting not only the customers but also adversely affecting the banks and the overall economy of a nation. Beyond monetary losses, non-monetary cybercrimes manifest when viruses are generated and spread on other computers or when confidential business information is exposed on the internet. Among these non-monetary crimes, phishing and pharming are particularly prevalent.[5]

The researcher seeks to identify the vulnerabilities of banking sector regarding cybersecurity in the face of cyberattacks and threats. By analysing the cyberattacks on banks, regulatory framework, and practices employed, the researcher aims to provide an in-detail understanding of the challenges faced and strategies employed.

**1.2 Statement of Problem:**

The swift digital evolution observed in the Indian banking sector, characterized by a significant rise in online transactions, mobile banking, and digital payment systems, poses a complex challenge. While it has undeniably enhanced customer accessibility and convenience, this transformation also introduces intricate vulnerabilities into the digital infrastructure. The evolving nature of this ecosystem becomes a fertile ground for cybercriminals, offering them fresh opportunities to exploit, thereby posing a threat to the strength, security, and integrity of the financial sector. It is crucial to address these challenges urgently to uphold the ongoing trust, dependability, and resilience of the Indian banking industry in light of the increasing threats from cybercriminal activities.

[4] "*2025 Digital Banking Fraud Trends in India*", https://www.biocatch.com/report-digital-banking-fraud-trends-india-2025#:~:text=Digital%20arrest%20scams%20rampant%3A%20The,focused%20on%20identifying%20mule%20accounts., (visited on September 10, 2025)

[5] Neeta, and V.K. Bakshi, "*Cyber Crimes In Banking Sector*", AAYUSHI INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL, Vol 4, May 2019, pp. 25.

### 1.3 Research Objectives

- To understand cybercrime and impact on Indian Banking sector.
- To study the legal mechanisms concerning cybersecurity.
- To analyse the issues and challenges faced by the Indian Banks in combating cybercrime.
- To give a roadmap for the Indian Banking Sector to enhance its cybersecurity.

### 1.4 Research Hypothesis:

The rapid digital transformation of the Indian banking sector, designed to enhance customer accessibility and convenience, simultaneously exposes opportunities for cybercriminals to exploit digital infrastructure vulnerabilities, posing challenges in the effective implementation of cybersecurity mechanisms by banks.

### 1.5 Research Questions:

- What is cybercrime and cybersecurity in the Indian banking sector and its impact?
- What are the legal provisions and regulatory bodies concerning cybercrime in India?
- What are the issues and challenges faced by the Indian Banks in the realm of cybersecurity?
- What could be the possible roadmap for the Indian Banking Sector by which it can improve its cybersecurity and resist cyberattacks?

### 1.6 Review of Literature

1. In the research article written by Seema Goel," Cyber-crime: A Growing threat to Indian Banking Sector",[6] the author has discussed he growth of web technology in the Indian banking sector and the increase in non-cash based transactions, highlighting the impact of the internet

[6] Seema Goel, "*Cyber-crime: A Growing threat to Indian Banking Sector*", International Journal of Science and Technology Management, Vol 5, 2016, pp. 552-558.

on the financial industry and also the existence of online fraud communities where stolen or leaked credit card numbers, online banking accounts, medical records, and administrative access to servers are traded for money, emphasizing the need for effective measures to combat such activities.

2. In the research article written by Manasi Sutar and Mayuri Talegaonkar, "Review of Cyber Security Threat in Banking Sector during Covid-19 Pandemic," [7] the author has discussed about the increasing availability of personal data with government and private sector players, posing a risk to Indians due to their lack of knowledge about security and privacy implications, the rise in cyber-attacks in India during the pandemic, indicating the need to address issues and challenges related to cybersecurity. And provided recommendations for securing cloud infrastructure, such as regularly assessing and updating cloud security, using multifactor authentication, and employing vulnerability management tools for threat detection.

3. In the article written by Simran Singhi and Vaishnavee Upreti "Corporate Governance and Cyber Security"[8] the authors highlight the continuous rise in technology and its impact on the business world, specifically the increased risk of cyber breaches. It emphasizes the importance of privacy and data management as core issues of corporate governance in India. The paper presents findings from a 2019 Chief Information Officer (CIO) survey, revealing that 69% of Indian organizations are at risk of data breaches. The authors discuss the provisions in Indian law that deal with cyber offenses, such as the introduction of the concept of phishing through a legal case.

4. In the research article by Dr. Neelam Sethi, "Cyber Security analysis in Banking Sector"[9], the author has analysed that cyber security in the banking sector is crucial due to the increasing risk of data breaches and cyber fraud. Cyber security is not solely a technological issue but requires expertise from various fields such as computer science, psychology, economics, and law. Banks need to consider the cyber protection of third-party providers to avoid potential security risks. Mobile apps pose a higher risk of attacks, and banking software solutions are

[7] Manasi Sutar and Mayuri Talegaonkar, "*Review of Cyber Security Threat in Banking Sector during Covid-19 Pandemic*", INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY, Volume 2, June 2022, pp. 368- 374.

[8] Simran Singhi and Vaishnavee Upreti "*Corporate Governance and Cyber Security*", INTERNATIONAL JOURNAL OF LAW) MANAGEMENT & HUMANITIES, Vol.4, 2021 pp.2808-2821.

[9] Neelam Sethi, "*Cyber Security analysis in Banking Sector*" INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMMERCE, MANAGEMENT & SOCIAL SCIENCE, Vol 04, July - September, 2021, pp. 59-64.

necessary to prevent unauthorized activities. Financial institutions are responsible for safeguarding sensitive customer information, and online transactions occur frequently, making information security a priority. Banks and financial organizations need to invest in advanced systems and technologies to go beyond preventing cyber attacks and ensure the security of data

5. In the research article by Neeta, "Cyber Crimes In Banking Sector",[10] the authors observed that while e-banking offers convenience and efficiency, it also poses risks in terms of cyber-crime. The liability of both banks and customers in cases of cyber-crime and suggests safeguards that should be undertaken by both parties while dealing electronically such as increase awareness among both banks and customers about the risks involved in e-banking and the necessary safeguard measures. Implement authentication, identification, and verification techniques for banking transactions in the electronic medium to prevent cyber-crime.

### 1.7 Rationale of the study:

As our environment has become more digital, more so after the Covid 19 pandemic, so do the risks to the security of our money and information in banks. The Indian banking sector, like others globally, faces constant threats from cyberattacks. Despite efforts to secure digital systems, challenges persist, and understanding them is crucial. This study is essential because by identifying and analyzing the issues hindering effective cybersecurity, we can develop targeted solutions. The main aim of this research is to find these issues, which can ensure the safety of financial transactions and protection of the sensitive data of the customers of Indian Banks.

### 1.8 Research Methodology

The methodology adopted by the researcher in this study is essentially doctrinal, explanatory and analytical, based on the analysis of both primary and secondary sources to understand cybercrime in Indian banking sector. The primary sources are the legislations, case laws and judgments. The secondary sources include books, newspaper editorials, official websites, articles and research papers published in various journals on the issue of cybercrime and cybersecurity in the Indian banking sector.

[10] Neeta and V.K. Bakshi, "*Cyber Crimes In Banking Sector*", AAYUSHI INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL, Vol 4, May 2019, pp. 25-31.

### 1.9 Scope and Limitations

The study encompasses the emerging cyber threats in the banking sector, the regulatory framework given by RBI and other laws which are to be followed by the Banking sector, the challenges faced by the Indian Banking Sector in regard to cybercrime. The limitation to this research is that the research is limited to the analysis of cybercrime and cybersecurity in Indian banking sector only, with focus on the cyberattacks and threats, the regulatory frameworks, issues and challenges.

## CYBERCRIME AND CYBER SECURITY

### 2.1. Introduction

In today's digital banking world, where technology has made banking easier and faster, there's a hidden challenge which is cybersecurity. Banks are vulnerable to cyber-attacks, which can lead to huge financial losses and data breaches. With the rising digitization of banking services, safeguarding the security of sensitive customer data and financial transactions is an important role of that banks need to play.

### 2.2 Cybercrime

There is no legal accepted definition of cybercrime. "One common definition describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity."[11] Cybercrimes are offences committed with a criminal motive against an individual or group to intentionally harm the reputation, cause physical/mental harm/loss, directly or indirectly using modern telecommunication networks.[12] Cybercrime is a classification of criminal actions primarily executed through computers and the internet. These malicious activities involve the deployment of malware and can lead to a range of adverse consequences. Instances include online stalking and identity theft, frequently resulting in substantial financial losses due to unauthorized withdrawals from victims' accounts.[13]

[11] "*Understanding cybercrime: a guide for developing countries*", https://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf, (Visited on October 18, 2023).
[12] *Jaydeep Vrujlal Depani v State of Gujarat* R/SCR.A/5708/2018 Order
[13] Medhansh Mishra And Raneeta Pal, "*The Rise in Cybercrimes: A Major Threat to Human Race",* INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES, Vol. 5, 2022, pp.1739

### 2.3 Cybercrime in Banking Sector

In the Indian context, banks have been facing persistent assaults from potential state and non-state actors, organized crime groups, and hacktivists. The frequency and intensity of these attacks emphasize the importance of developing and implementing robust cybersecurity measures to safeguard the integrity and confidentiality of financial systems in India.[14] Cyberattacks pose a significant threat to the banking sector due to the valuable information and assets they possess. With the widespread use of mobile devices and web apps, ensuring cybersecurity in banking is crucial to protect consumers online. Banks need to prioritize security to gain customer trust, especially in the constantly evolving landscape of cybersecurity threats. [15] Further "the right to privacy is a fundamental right, and that individuals have the right to protect their data from cyber threats"[16].

The Reserve Bank of India has said that the banks should focus on fortifying cyber security and prevention of cyber frauds to safeguard their customers from rising incidents of fraud and data breaches.[17] UCO Bank, a public sector lender based in Kolkata, disclosed an inadvertent crediting of Rs 820 crore to its account holders through the Immediate Payment Service (IMPS). Between November 10 and 13, the bank identified technical glitches in IMPS, leading to specific transactions initiated by account holders from other banks incorrectly resulting in the crediting of funds to UCO Bank account holders without the actual transfer of money from these external banks. [18] These instances shows that banks are under a constant threat from the cyber attacks and highlight the need to have good cybersecurity mechanisms.

---

[14] Nandkumar Saravade, "*Ambuj Bhalla, Emerging trends and challenges in cyber security*" https://rebit.org.in/ReBIT/whitepaper/emerging-trends-and-challenges-cyber-security, (visited on September 10, 2025).

[15] "*Significance of cybersecurity in Indian banking system",* https://primelegal.in/2023/06/11/significance-of-cybersecurity-in-indian-banking-system/#:~:text=Banking%20cybersecurity%20solutions%20include%20network,frequent%20security%20evaluations%20and%20testing, (visited on October 1, 2023).

[16] *K.S. Puttaswamy (Retd.) and Another vs. Union of India,* AIR 2017 SC 4161

[17] IANS, Stock Market News, "*Banks should fortify cyber security as fraud cases rise: RBI"*, November 23, 2023, https://in.investing.com/news/banks-should-fortify-cyber-security-as-fraud-cases-rise-rbi-3911446, (visited on October 1, 2023).

[18] Swati Nair, "*Finance Ministry calls meet to discuss digital payment fraud, cyber security",* https://www.goodreturns.in/news/finance-ministry-calls-meet-to-discuss-digital-payment-fraud-cyber-security-gen-1314237.html, (visited on October 1, 2025).

### 2.4 Cybersecurity in Banking Sector

Cybersecurity means "how individuals and organisations reduce the risk of cyberattack."[19] Banks have to maintain secrecy of customers account.[20] This obligation dates back to 1924 where in a case[21] in which it was held Banks are required to maintain strict confidentiality regarding a customer's financial status and account details to prevent harm to the customer's reputation, creditworthiness, and business. The emergence of new technology has made upholding this obligation challenging, as hackers can gain unauthorized access to accounts, complicating the task of ensuring customer privacy. In Apple v. FBI, apple was asked to create a unique OS just to open the accused's phone but apple refused stating "in the wrong hands, this software which does not exist today would have the potential to unlock any iPhone in someone's physical possession."[22] Facing a cyber-attack not only jeopardizes a bank's reputation but also translates into financial losses for its clients, with the recovery process being notably prolonged in cases of information breaches. Customer trust is eroded when a bank's cybersecurity measures prove vulnerable, emphasizing the paramount importance of robust security protocols for safeguarding critical data. In the digital age, where virtually all aspects of life are digitized, banks must enhance their capabilities to meet customer needs. The swift access that hackers can gain to banking apps highlights the urgency for financial institutions to prioritize and implement effective cybersecurity strategies, ensuring the security of both customer information and the overall integrity of the banking system.[23]

### 2.5 Types of Cybercrime

With the technological advancement there has also been an increase in cyber risks by organizations being more prone to cyberattacks, with the cyberattacks comes the risk of data breaches. The expansion of digital financial services has increased financial inclusion but also raised cybersecurity concerns. [24] Data breaches are increasingly common in the

[19] "*What is cyber security*?", https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security, (visited on October 3, 2023).
[20] Section 13 of Banking Companies (Acquisition and Transfer of Undertaking) Act 1970.
[21] *Tournier v. National Provincial & Union Bank of England*, (1924), K.B., 461.
[22] *United States v. In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD20*3, 5:16-cm-00010, C.D. Cal.
[23] Manasi Sutar and Mayuri Talegaonkar, "*Review of Cyber Security Threat in Banking Sector during Covid-19 Pandemic*", "INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY", Volume 2, June 2022, pp. 369.
[24] Mohd Adhari, "*Belal Din: Cybersecurity – safeguarding the future for innovative financial inclusion*", https://www.bis.org/review/r170814e.pdf, (visited on October 3, 2023).

corporate world, making it essential to address cybersecurity issues. While developed nations were traditionally targeted, Indian companies are now equally vulnerable to cyberattacks.[25] A recent report by Kearney suggests that cybersecurity has been a key issue amongst almost every organization and that cyber-attacks have been at the top of the list of business risk for three consecutive years.[26] The kinds of privacy threats and risks are very vast in number and do not fail in keeping up with the technological changes. The type of cybercrime that the Indian baking institutions face are as follows[27]:-

**2.5.1. Malware –** Its a cyber-attack that involves malicious software being installed in a system, appearing as legitimate software and granting unauthorized access without the user's knowledge. It infiltrates through methods like email attachments or software downloads.

**2.5.2. Ransomware -** This type of malware encrypts a user's system, making it inaccessible until a ransom is paid to the attacker. It's an advanced and highly dangerous cyberattack. This affects transparency as banks may not be able to openly disclose the full extent of the attack and can impact the reputation of the banks.

**2.5.3. Phishing** - In this type of attack, a deceptive web page or email resembling an authentic source is created to lure users into clicking the link. The goal is to obtain personal and sensitive data like login credentials, credit card numbers. The Delhi High Court defined phishing as "…a form of internet fraud…"[28]. This also includes vishing, a form of phishing conducted via phone calls, where fraudsters use telephones to deceive users into divulging private information for fraudulent activities.[29] It can have a devastating impact as it can used to gain a foothold in the institution's network and launch a larger attack like an advance persistent threat.[30]

**2.5.4. DDoS:** Under Distributed Denial of Service (DDoS) attacks the system gets overloaded with requests to access the server and ultimately resulting in the server being crashed. If a DDoS attack disrupts services, the bank is held responsible for the failure, affecting its

[25] Simran Singhi and Vaishnavee Upreti "*Corporate Governance and Cyber Security*", INTERNATIONAL JOURNAL OF LAW) MANAGEMENT & HUMANITIES, Vol.4, 2021, pp.2809.
[26] Raman Shankar, "*Corporate governance in banking sector in India: An analytical study*", - JOURNAL OF MODERN MANAGEMENT & ENTREPRENEURSHIP, Vol. 10, July, 2020
[27] Supra Note 25 p.2810.
[28] *National Association of Software and Services Companies v. Ajay Sood* 2005 (30) PTC 437 (Del).
[29] Vishing, SBI, https://sbi.co.in/web/personal-banking/cyber-security#:~:text=To%20report%20any%20cyber%20incident,cyber%20crime%20helpline%20number%201930. (visited on October 9, 2023).
[30] "*Fundamentals of Cybersecurity in Banks*", https://www.qentelli.com/thought-leadership/insights/fundamentals-cybersecurity-banks, (visited on October 9, 2023).

accountability. If the attack creates discrepancies in service availability, fairness in customer treatment can be compromised. Failing to protect against DDoS attacks indicates a breach in fulfilling this responsibility, potentially eroding customer trust in the bank's ability to provide reliable services.

**2.5.5. Smishing:** This type of attack employs text messages sent to cell phones, resembling phishing techniques. These messages, appearing to be from genuine sources, are often combined with other methods to bypass built-in protections. Victims might be redirected to malicious websites on their phones.[31]

**2.5.6 Credit Card Fraud:** Cybercriminals take advantage of the rise in online transactions, particularly focusing on 'card-not-present' (CNP) fraud. In this type of fraud, they make unauthorized purchases without the physical presence of the card. Criminals acquire victim information through phishing attacks or by acquiring data through purchases on the darknet.

**2.5.7. Deepfakes**: With India's financial sector rapidly digitizing, deepfakes have emerged as a serious new threat. Recent scams—ranging from a Kerala man losing ₹40,000, a woman duped of ₹1.4 lakh through an AI voice call, to a ₹5 crore fraud using AI face-swapping—highlight the scale of the problem. Powered by AI, deepfakes can convincingly manipulate voices and faces, making them powerful tools for fraudsters. Their misuse in processes like Video KYC exposes banks and financial services to major risks, turning what could be a creative technology into a weapon for large-scale financial crime.[32] The surge in deepfake fraud is fueled by generative AI, which has become cheap and easy to use, allowing criminals to produce realistic fakes without much skill. This makes large-scale scams in banking easier to pull off. The real concern is that traditional fraud detection often can't keep pace with these fast-evolving techniques. Even AI-based security tools used by banks need constant upgrading to outsmart increasingly sophisticated deepfakes.[33]

[31] Supra Note 25 p.2010.
[32] "*How do deepfakes impact banks and other financial institutions*?", December 26, 2023, Financial Express, https://www.financialexpress.com/money/how-do-deepfakes-impact-banks-and-other-financial-institutions-3347654/,(visited on October 8, 2023).
[33] "*How Deepfakes Can Be Used to Commit Banking Fraud*", https://www.hdfcbank.com/personal/resources/learning-centre/vigil-aunty/how-deepfakes-can-be-used-to-commit-banking-fraud, (visited on October 5, 2023).

### 2.6 Cyberattacks

Following are some of the big cyberattacks that happened to Indian banks[34]:-

**2.6.1. India's largest Data Breach:** In 2016, a major data breach occurred in India's banking sector, affecting 3.2 million debit cards from banks like SBI, HDFC, ICICI, YES Bank, and Axis Bank. Attackers injected malware into Hitachi Payment Services' payment systems, stealing both debit card numbers and PINs. SBI blocked and re-issued 600,000 affected cards, making it the largest data breach in Indian banking history.

**2.6.2. Union Bank of India Hacked:** In 2017, Union Bank of India fell victim to a phishing attack when an employee opened a malicious email, leading to a malware attack. Hackers gained access to the bank's network, stole access codes for international transactions through SWIFT, and transferred $170 million to a Citigroup account in New York.

**2.6.3. Cosmos Cooperative Bank Attack:** In 2018, Cosmos Cooperative Bank faced a malware attack on its ATM servers for 2 days, resulting in the loss of Rs 94.42 crore. Debit cards were cloned, and 15,000 ATM transactions occurred within seven hours, laundering Rs 80.5 crore. Another Rs 13.92 crore was transferred to a Hong Kong-based firm via SWIFT the next day.

In early 2024, a leading Indian bank fell victim to a highly sophisticated AI-driven phishing attack that exposed the limitations of traditional cybersecurity. The attackers used advanced natural language processing to mimic executives' writing styles and communication patterns, creating spear-phishing emails that appeared authentic and directed recipients to a fake internal portal. Senior managers unknowingly shared their login credentials, giving criminals access to sensitive databases and disrupting banking operations for days. The attack combined technical precision with human manipulation, exploiting trust, authority, and urgency while evading detection through dynamic content changes, polymorphic code, and phantom domains. Beyond financial and operational losses, the incident dealt a long-term reputational blow to the bank, highlighting how AI enables cybercriminals to merge technology with social engineering in

[34] "*Cybersecurity priorities of the Indian banking industry post pandemic*", https://download.manageengine.com/images/indian-banking-industry-39s-cybersecuritywhitepaper.pdf?pos=BFSI (visited on October 8, 2023).

ways that outpace existing defenses.[35]

Thus, as illustrated by real-world examples in the Indian context, cybercrimes such as data breaches, phishing attacks, and malware intrusions pose significant threats to the security and integrity of banking systems. The imperative for robust cybersecurity measures is emphasized not only by the financial losses incurred but also by the potential compromise of sensitive customer data. As the banking sector navigates the ever-evolving landscape of cyber threats, the safeguarding of customer trust and data privacy remains paramount, requiring continual adaptation to emerging technologies and proactive measures against cyber adversaries.

## REGULATORY FRAMEWORK

### 3.1 Introduction

In the rapidly evolving landscape of the Indian banking sector, cybersecurity stands as a critical cornerstone underpinning trust and financial stability. As the industry navigates the digital era, the need for a robust legal framework and policies to combat cyber threats is imperative. This chapter delves into the intricate legal structures governing cybersecurity within the Indian banking sector.

### 3.2 Laws regarding Cybersecurity for Banks:-

**3.2.1 Reserve Bank of India:** The RBI has the duty to act in the interest of the public at large and with transparency[36]. It has issued circulars and master direction regarding cybersecurity framework of banks including urban cooperatives banks, NBFC. These are Cyber Security Framework 2016, Basic cybersecurity framework for Urban Cooperative Banks 2018, Information Technology Framework for the NBFC Sector 2017.

**3.2.1.1 Cyber Security Framework**: Bank's cybersecurity policy should be different from the broader IT/IS security policy and should be based on regular vulnerability testing and the establishment of a Security Operations Centre (SOC). Banks should design their IT architecture to facilitate continuous security measures and have the IT Sub Committee of the Board review

[35] "*Research Report: AI-Driven Phishing Attack on a Financial Institution in India (2024)*" https://www.cyberpeace.org/resources/blogs/research-report-ai-driven-phishing-attack-on-a-financial-institution-in-india-2024, (visited on October 7, 2025)

[36] *Reserve Bank of India v. Jayantilal N. Mistry,* (2016) 3 SCC 525.

and upgrade it based on risk assessments. A minimum baseline cybersecurity and resilience framework is required, including the setup and operation of a SOC and the development of a Cyber Crisis Management Plan. Banks should proactively prevent and detect cyber threats, including emerging threats like zero-day attacks and ransomware. Information sharing and participation in cybersecurity forums are encouraged. Cybersecurity awareness and training are essential for managing cyber risk, promoting a synchronized implementation and testing approach.[37]

The RBI Circular also had 3 annexures with provided that banks need to have a cybersecurity and resilience which contains an indicative list of information security information and cybersecurity preparedness that banks must follow, setting up of cybersecurity operation(C-SOC) and cyber security incident reporting(CSIR). The Cyber Security Framework in Banks requires banks to inform the RBI of any cybersecurity incident within two to six hours of the breach and include details of it in a standard reporting template.[38]

**3.2.1.2 Basic cybersecurity framework for Urban Cooperative Banks:** Under which UCBs are required to develop a Board-approved Cyber Security Policy distinct from their IT/IS policy, considering the level of technology adoption and digital products offered. The policy should address cyber threats and outline security measures. UCBs must ensure their IT architecture is security compliant, establish a Cyber Crisis Management Plan, detect and respond to cyber intrusions, raise organizational awareness, protect customer information, and promptly report cybersecurity incidents to the regulatory body. [39]

**3.2.1.3 Master Direction** - Information Technology Framework for the NBFC Sector: These guidelines cover various aspects of IT governance, IT policy, information and cyber security, IT operations, IS audit, business continuity planning, and IT services outsourcing. For NBFCs with asset size above ₹500 crore, the guidelines emphasize the formation of an IT Strategy Committee, development of robust IT policies, implementation of information security measures, and conducting regular IT audits. For smaller NBFCs with asset size below ₹500 crore, the guidelines recommend starting with basic IT systems that include fundamental

[37] "*Cyber Security Framework in Banks*", https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0 (visited on October 7, 2023).
[38] Supra Note 37.
[39] "*Cyber Security Framework in Banks*", https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0 (visited on October 8, 2023).

security aspects, user role definition, maker-checker concept, information security, and compliance with regulatory requirements.[40]

Banks need to strictly adhere to these directions as non-compliance can lead to imposition of penalty as in the case of AP Mahesh Cooperative Urban Bank where RBI fined it 65 lakh rupees due to their failure to comply with the Cyber Security Framework for Cooperative Banks. In January 2022, hackers stole 12.48 crore rupees after breaching APMCUB's security systems[41]. Another instance is YES Bank being fined Rs 6 crore by the RBI for not reporting a cybersecurity breach in its ATM network and for violating regulations related to Income Recognition Asset Classification (IRAC).[42] The RBI also imposed a fine of Rs.5.39 crore on Paytm Payment Banks for violating KYC norms.[43]

Know Your Customer (KYC) mandated by RBI, assures customers of compliance and anti-fraud measures, ensuring secure payment processing and establishing trust. RBI guidelines, u/s 45K[44] and 45L[45] of the RBI Act, 1934 and Rule 7[46] of Prevention of Money-Laundering Rules, enforce strict adherence. Non-compliance may result in monetary penalties of ₹2 lakh for banks, businesses, and corporations.

### 3.2.2 The IT Act and the Information Technology (Amendment) Act 2008

The IT Act contains provisions for the protection of electronic data. The IT Act penalises 'cyber contraventions' (section 43(a)–(h)) and 'cyber offences' (sections 63–74). It also addresses data protection and cybersecurity concerns. The IT Act and Rules do not explicitly address the issue of breach of directors' or officers' duties, but individuals in charge of the company's business, such as directors and officers, will be held accountable in case of violation

[40] "*Master Direction - Information Technology Framework for the NBFC Sector*", https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10999 (visited on October 7, 2023).

[41] "*RBI slaps Rs 65 lakh penalty on bank for hacking breach*", Times of India, http://timesofindia.indiatimes.com/articleshow/101425742.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, (visited on October 15, 2023).

[42] Riddhi, "*MukherjeeRBI Fines YES Bank For Failing To Report Cyber Security Attack On Its ATM Network*", https://www.medianama.com/2017/10/223-rbi-fines-yes-bank-failing-report-cyber-security-attack-atm-network/, (visited on October 15, 2023)

[43] "*RBI imposes Rs 5.39 cr penalty on Paytm Payments Bank for KYC norms violation*", https://www.moneycontrol.com/news/business/rbi-imposes-rs-5-39-cr-penalty-on-paytm-payments-bank-for-kyc-norms-violation-11522081.html, (visited on October 15, 2023).

[44] Section 45K. The Reserve Bank of India Act, 1934 (Provides Power of Bank to collect information from non-banking institutions as to deposits and to give directions.

[45] Section 45L. The Reserve Bank of India Act, 1934 (Provides Power of Bank to call for information from financial institutions and to give directions.

[46] Rule 7 PML (Maintenance of Records) Rules 2005 (Provides Procedure and manner of furnishing information.

of provisions of the Act.[47]. They can be charged and penalized for the violation. Companies and organizations are required to maintain "reasonable security practices and procedures" to safeguard crucial information from compromise, damage, exposure, or misuse and when they do not adopt acceptable security measures for safe banking are required to provide adequate compensation to customers[48]. The complaint's email account was purportedly hacked, and private information about the complainant's bank account was disclosed. Due to SBI's negligence in providing the complainant's bank account details, it was determined that the bank was required by Act 43A to compensate the complaint[49]. In[50], it was decided that the bank violated sec. 43 of the IT Act by failing to take reasonable precautions to prevent an unauthorized entry, and as a result, the bank was required to compensate the complainant.

Sec. 72A of the Act criminalizes the unauthorized disclosure of personal data without the owner's consent, imposing penalties of imprisonment up to three years, a fine of up to Rs500,000, or both for those found guilty. The IT Act, 2000 provides for prescriptive jurisdiction as u/s 75[51] the provisions of the Act will apply to any offence or contravention which is committed outside India by any person regardless of his nationality. It also applies if the offense or violation involves a computer, computer system, or computer network situated in India. A statute extends territorially unless a contrary is stated, throughout the country and will extend to the territorial waters and such places as intention to such places is shown.[52] "To prove a prima facie case that plaintiff will need to prove defendant engaged in some commercial activity in the Forum State by targeting its website specifically at customers within that State."[53]

A person who is a victim of online banking fraud can file a complaint with the Adjudicating Officer under Section 46 of the Act, alleging that the bank failed to implement appropriate security measures.

**3.2.3 Information Technology Rules 2011:** The IS/ISO/IEC 27001 regulations, recognized by the Indian SPDI Rules of 2011, are international standards that Indian companies are not legally

[47] Section 85 of the Information Technology Act, 2000.
[48] Section 43A of the Information Technology (Amendment) Act 2008.
[49] *State Bank of India v. Chander Kalani and Others*, 2019 SCC OnLine Del 7031.
[50] *Umashankar Sivasubramanian v. ICICI Bank* , Civil Jurisdiction Petition No. 2462 of 2018.
[51] Section 75 of Information Technology Act 2000 (provides Act to apply for offence or contravention committed outside India).
[52] *British India Steam Navigation Co. ltd. v Shanmughavilas Cashew Industries*, AIR 3 SCC 481.
[53] *Cybersell Inc. v. Cybersell Inc.,* 130 F 3d 414.

obligated to follow but are strongly recommended to adopt. It requires entities holding users' sensitive personal information to maintain certain specified security standards. [54]

**3.2.4 The Digital Personal Data Protection Act 2023:** The DPDP aims to safeguard data principals and regulate data fiduciaries. Under this, data fiduciaries must adhere to several obligations, including appointing third-party data processors who follow DPDP procedures, ensuring accuracy of personal data, maintaining compliance measures, implementing security safeguards, and promptly notifying affected parties. Financial companies can improve data security, win their customers' trust, and show responsible data management by adopting the Act. [55] While granting individuals rights over their personal data, carves out key exemptions for law enforcement purposes. Individuals cannot withdraw consent or restrict data use when their information is processed by the State for investigations or prosecutions. This exception reflects the ongoing tension between ensuring effective crime control and safeguarding personal privacy, underscoring the need for balanced legal safeguards that uphold both enforcement efficiency and citizens' data rights.[56] In today's data-driven world, adhering to the Act helps them to manage changing requirements and establish themselves as data custodians.[57]

**3.2.5 Companies (Management and Administration) Rules, 2014:** The managing director, company secretary, or any other director or officer of the company is in charge of maintaining and safeguarding electronic documents, according to rule 28[58] of the CAM Rules. He must take all necessary steps to ensure the security, integrity, and confidentiality of records, furthermore, he must make sure that computer systems, software, and hardware are secured and validated to

[54] Rohan Bagai, "*Aprajita Rana, Shagun Badhwar, Sana Khan, Cybersecurity 2021 – India Chapter*", https://www.azbpartners.com/bank/cybersecurity-2021-india-chapter/ (visited on October 8, 2023)

[55] "*Explainer: How Digital Personal Data Protection Act of 2023 will impact financial sector*", The Economic Times, https://bfsi.economictimes.indiatimes.com/news/financial-services/explainer-how-digital-personal-data-protection-act-of-2023-will-impact-financial-sector/103558476#:~:text=By%20embracing%20the%20DPDPA%2C%20financial,an%20increasingly%20data%2Ddriven%20world. (visited on October 14, 2023).

[56] Sajai Singh, et. al., "*Stringent measures against cybercrimes in India's new criminal justice system*", https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system/#:~:text=A%20key%20introduction%20in%20the,a%20member%20or%20on%20behalf

[57] Explainer: How Digital Personal Data Protection Act of 2023 will impact financial sector, https://bfsi.economictimes.indiatimes.com/news/financial-services/explainer-how-digital-personal-data-protection-act-of-2023-will-impact-financial-sector/103558476#:~:text=By%20embracing%20the%20DPDPA%2C%20financial,an%20increasingly%20data%2Ddriven%20world. (Visited on October 14, 2023).

[58] "*Cybersecurity 2021 – India Chapter*", https://www.azbpartners.com/bank/cybersecurity-2021-india- chapter/, (visited on October 7, 2023).

ensure their accuracy, reliability, and accessibility. Any such employee's failure in this regard could be interpreted as a violation of their obligations to the organization. [59]

The new criminal law framework—comprising the *Bharatiya Nyaya Sanhita (BNS)*, *Bharatiya Nagarik Suraksha Sanhita (BNSS)*, and *Bharatiya Sakshya Adhiniyam (BSA)*—marks a significant transformation in India's approach to technology and crime. It formally recognises cybercrime and economic offences as part of organised crime, thereby prescribing stricter penalties for coordinated, technology-driven criminal activities. The *BNSS* introduces key procedural reforms by enabling electronic service of summons, audio-video recording of statements, and digital documentation of search and seizure operations. Trials, inquiries, and appeals may now be conducted electronically, enhancing efficiency and transparency in cybercrime investigations. Substantively, the *BNS* broadens the scope of several offences—such as extortion, forgery, hate speech, and obscenity—to include acts committed through digital platforms. Provisions under **Sections 196–197** (hate speech), **Section 353** (misinformation and fake news), and **Section 294** (obscene digital content) explicitly extend to online communications, aligning with the *Information Technology Act, 2000* to ensure accountability for online offences. Complementing this, the *BSA* strengthens evidentiary procedures by granting **electronic records the status of primary evidence under Section 57**, while **Section 63** mandates authentication and certification to prevent manipulation. Collectively, these reforms modernise India's criminal justice system by integrating technology across all stages—from investigation to trial—while emphasising the need for robust data protection and cybersecurity measures to safeguard digital records and uphold public trust. [60]

### 3.3 Regulatory Bodies

**3.3.1 Computer Emergency Response Team (CERT-In):** It is India's national nodal agency for handling cybersecurity incidents. It require Indian companies to report incidents within six hours, non-compliance can result in imprisonment and fines.[61] Rule 12 of the CERT-In Rules prescribes the operation of a 24-hour Incident Response Helpdesk. Any individual,

[59] Supra Note 51.
[60] Sajai Singh, et. al., "*Stringent measures against cybercrimes in India's new criminal justice system*", https://www.jsalaw.com/newsletters-and-updates/stringent-measures-against-cybercrimes-in-indias-new-criminal-justice-system/#:~:text=A%20key%20introduction%20in%20the,a%20member%20or%20on%20behalf
[61] "*CERT-In*", https://www.cert-in.org.in/, (visited on October 5, 2023).

organisation or corporate entity affected by cybersecurity Incidents may report the Incident to Cert-In.

**3.3.2 Critical Information Infrastructure Protection Center (NCIIPC):** It serves as India's national agency for safeguarding critical information infrastructure. Its role involves monitoring and reporting national-level threats to crucial sectors such as power, banking, telecommunications, transportation, government, and strategic enterprises[62].

**3.3.2 Securities and Exchange Board of India:** It functions as the regulatory authority for India's securities and commodity markets and ensures the protection of market intermediaries, investors, and securities issuers, including safeguarding their data and transactions. SEBI has an eight-member committee called the High-Powered Steering Committee on Cybersecurity overseeing cybersecurity initiatives in line with global standards and a seven-member committee called Information Systems Security Committee to take immediate action on cyber security incidents. It collaborates with agencies like CERT-In, NCSC, DoT, and MeitY. Non-compliance penalties, such as violating disclosure regulations, incur a daily fine of ₹20,000 until compliance is met.[63] It has the jurisdiction to investigate and regulate companies even if they are not listed on stock exchange.[64]

### 3.4 Enforcement Actions in case of Non- Compliance

Banks need to strictly adhere to these directions as non-compliance can lead to imposition of penalty as in the case of AP Mahesh Cooperative Urban Bank where RBI fined it 65 lakh rupees due to their failure to comply with the Cyber Security Framework for Cooperative Banks. In July 2021, the Reserve Bank of India (RBI) levied a fine of INR 50 million on Axis Bank, one of India's major private banks, for violating provisions within its cybersecurity framework. Around the same time, RBI imposed a penalty of INR 2.5 million on Punjab & Sindh Bank, a nationalized bank, for comparable violations. This action followed the bank's report of several cyber incidents to the RBI in May.[65] In January 2022, hackers stole 12.48 crore rupees after breaching APMCUB's security systems[66]. Another instance is YES Bank being fined Rs 6 crore

[62] Supra Note 58.
[63] "*Securities and Exchange Board of India*", https://www.sebi.gov.in/, (Visited on October 8, 2023).
[64] *Sahara India Real Estate Corporation Limited and Others v. Security and Exchange Board of India Civil* Appeal No. 9813/2011.
[65] "*Investigation Cybersecurity Laws and Regulations India 2023'*, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india, (visited on November 4, 2023).
[66] Supra Note 41.

by the RBI for not reporting a cybersecurity breach in its ATM network and for violating regulations related to Income Recognition Asset Classification (IRAC).[67] The RBI also imposed a fine of Rs.5.39 crore on Paytm Payment Banks for violating KYC norms.[68] RBI has the authority to impose penalty to the banks under section 47A[69] of the Banking Regulation Act, 1949.

**3.5 Case Study:**

**3.5.1. Pune Citibank Mphasis Call Centre Fraud:** In 2005, 3,50,000 dollars were fraudulently transferred from their bank accounts in Citibank into few bogus accounts based in U.S. this act was done by employees of call center. They won the confidence of the customers by pretending to help them with their issues relating to their bank accounts and obtained their PIN and used it transfer the money to some bogus account. The two main issue were whether this offence constituted a cybercrime and whether sec.43(a) and sec. 66[70] was applicable. The court held that since the act involved unauthorized access to the electronic accounts of the customers, it fell under the ambit of cybercrime and was to be dealt by IT Act, 2000. The accused was charged under sec 43(a) and 66 of the Act and also under IPC. This case highlighted the importance of having stricter data protection laws in India so that cybercriminals could be dealt with in a stricter manner.[71]

**3.5.2. The Bank NSP Case:** In this case, a trainee employed by the bank, who was engaged with a colleague, communicated extensively via company computers. Following their breakup, the girl, using the bank's computer, created deceptive email accounts like "indianbarassociations" and sent fraudulent emails to the boy's international clients. This action resulted in a substantial loss of clients for the boy's company, leading to a legal dispute where the bank was held liable for the emails sent through its system.[72]

[67] Supra Note 42.
[68] RBI imposes Rs 5.39 cr penalty on Paytm Payments Bank for KYC norms violation, Money Control New, October 2, 2023.https://www.moneycontrol.com/news/business/rbi-imposes-rs-5-39-cr-penalty-on-paytm-payments-bank-for-kyc-norms-violation-11522081.html, (visited on October 15, 2023).
[69] Section 47A Power of Reserve Bank to impose penalty, The Banking Regulation Act, 1949.
[70] Section 66 of the Information Technology Act 2000, (provides computer related offences).
[71] Talwant Sigh, "*Cyber Law and Information Technology*", https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf, (Visited on November 4, 2023).
[72] Ibid.

### 3.6 Cybersecurity: Legislation Overview

Countries like the USA and Israel are at the top in terms of cybersecurity mechanisms to combat cybercrimes in their countries. They have specific laws regarding data protection, privacy and critical infrastructure. In India also there is legislation on data protection and privacy under the new Act Digital Personal Data Protection Act 2023, but India lacks a legislation in critical infrastructure which is the most important of all.[73] Though it has a nodal agency for taking measures to protect the nation's critical information infrastructure called National Critical Infrastructure Protection Centre. But it has not defined explicitly the critical infrastructures in its policy documents.[74] Other countries like Germany and the UK are also doing better than India. They use the defensive approach in their cybersecurity strategy and are able to protect their valuable assets and have successfully been able to protect their resources from complex, volatile, uncertain cyber threats in comparison to other countries.[75]

India's banking sector faces growing cybersecurity challenges in the digital age, making robust legal provisions and policies essential. The RBI has issued guidelines mandating banks to establish comprehensive cybersecurity policies, focusing, secure IT architecture, and incident reporting. The Information Technology Act, 2000, and the Digital Personal Data Protection Act of 2023 provide legal structures to safeguard sensitive information, ensuring compliance through penalties and fines. Various regulatory bodies, including CERT-In, NCIIPC, and SEBI, oversee cybersecurity enforcement, emphasizing the critical importance of adherence to regulations and standards.

## ISSUES AND CHALLENGES

Indian consumers are increasingly gravitating towards online services, drawn by the allure of convenience, cost-effectiveness, and the rapidity of digital transactions. Financial institutions are also actively promoting cashless transactions by offering enticing deals, leveraging the relatively lower operational costs associated with such transactions. However, it becomes evident that the cybersecurity measures implemented by financial institutions to combat

[73] Nuruddin Khan, Dr. Shobha Gulati, "*International Legislative Framework Of Cybercrimes- A Comparative Study Of India, Israel, And USA*", JOURNAL OF POSITIVE SCHOOL PSYCHOLOGY, Vol. 7, 2023, pp. 789.
[74] Prashant Mali, "*Critical Analysis of Cyber Security Policies of USA, UK, India and Germany*", 2015, https://www.academia.edu/27332064/Critical_Analysis_of_Cyber_Security_Policies_of_USA_UK_India_and_Germany, (visited on November 10, 2023).
[75] Ibid.

cybercrime are struggling to keep pace with the dynamic technological landscape and the enhanced proficiency of cyber intruders.[76]

### 4.1 Current State of Cybercrime in Banks:

Between June 2018 and March 2022, Indian banks experienced 248 successful data breaches, with the government reporting 11,60,000 cyber-attacks in 2022, three times more than in 2019. Notable attacks include a 2016 phishing attempt at Union Bank of India almost resulting in a $171 million fraudulent transaction[77]. CloudSEK, a cybersecurity firm, revealed that 7.4% of targeted attacks in 2022 focused on the Indian subcontinent. India, ranking third in global internet user numbers, has become a major target for cyber-attacks, involving nationalized banks, crypto exchanges, NBFCs, and credit card information leaks. [78] In a case[79] involving the Maharashtra IT department, Punjab National Bank was ordered to pay Rs 45 lakh to the complainant as he was defrauded when he responded to a phishing email, resulting in a transfer of Rs 80.10 lakh from his PNB account in Pune. The bank was deemed negligent because it failed to conduct security checks on fraudulent accounts, leading to the fraudulent transfer.

### 4.2 Issues and Challenges

Following are the issues and challenges faced by the Indian Banks in cybersecurity which impacts the corporate governance of the banks:-

**4.2.1 Issue of Jurisdiction:** When a state has prescriptive jurisdiction then its jurisdiction is unlimited and it can legislate for any matter irrespective of where it occurs or the nationality of the persons involved but has no jurisdiction to adjudicate, like u/s 75 of the IT Act, 2000 extends the Act's applicability to offenses committed outside India involving Indian computer systems. While the Act prescribes laws for non-residents, the challenge lies in adjudication, especially if extradition is necessary. Non-residents often do not agree to the jurisdiction of the regulating state and the foreign courts might not enforce judgments made by Indian courts under the IT Act due to differences in legal interpretations. In cases involving foreign nationals

[76] Supra Note 6 p.553.
[77] Zeshan Naz, "*Cyber Security in Banking*", https://www.knowledgehut.com/blog/security/cyber-security-in-banking (visited on October 7, 2023).
[78] Tanushree Basuroy, "*Incidents of cyberattacks across India from 2015 to 2022*", https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks/ (visited on October 9, 2023).
[79] *Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others,* Complaint No. 4 of 2011 dated 9/11/2011.

committing offenses under the IT Act, cooperation and legal assistance are essential from authorities in the foreign country where the individual resides. Obtaining such cooperation is challenging without international agreements like a Cybercrime Convention or Mutual Legal Assistance Treaty (MLAT), both of which India has not signed[80]. Although India has signed some MLATs for general criminal matters, they may not cover cybercrime adequately. Additionally, India's current agreements, like the UN Convention Against Transnational Organized Crime, might not effectively address cybercrime cases.

**4.2.2 Compliance of Legal Provisions:** One of the sectors with the highest levels of regulation is banking. It takes a substantial time and resource to ensure and maintain compliance with all relevant rules and legislation. Online Banking is governed by various laws like the IT Act 2000, RBI Act 1934, Digital Personal Data Protection Act 2023 etc. There is no harmonized framework which creates challenges in ensuring effective regulation of online banking.[81] The best example can be seen through the new digital personal data protection Act 2023. Under this, the banks have to provide a notice to its customers seeking consent for processing their data[82]. While the customers now have the right to withdraw consent but the banks now have to see that there is ease of withdrawal of consent and banks are not unaware of it, along with that they have to comply with the RBI's guidelines, which adds another layer of complexity. Banks have to see that the personal data is erased not only on consent but also it is reasonable to assume that the specified purpose is no longer being served[83]. There is lack of clarity on what is specified purpose no longer being served. Furthermore, banks need to balance these requirements with other data retention requirements under other laws, such as RBI's KYC Direction of 2016, which mandates that transaction records of last 5 years be kept in record[84]. This complexity poses challenges for banks in navigating compliance while ensuring data integrity and customer expectations.[85] Failures to comply can have severe consequences such as severe fines. For banks, maintaining regulatory compliance has become very difficult. The

[80] "*India and the Budapest Convention: why not?*", https://rm.coe.int/16806a6698, (visited on October 15, 2023).
[81] Madhura Pitre , "*Critical analysis of legal framework regulating internet banking in India*", INDIAN JOURNAL OF INTEGRATED RESEARCH IN LAW, Vol 3, 2022, p. 13.
[82] Section 5 of the Digital Personal Data Protection Act,2023(provides Notice).
[83] Section 8(7)(a) of the Digital Personal Data Protection Act,2023.
[84] "*Master Direction - Know Your Customer (KYC) Direction*", 2016, N0.46-Record Management.
[85] Arjun Goswami, "*India's new data protection law: Here's how the landmark law can impact the country's financial services sector*", Business Today, August 24,2023, https://www.businesstoday.in/opinion/columns/story/indias-new-data-protection-law-heres-how-the-landmark-law-can-impact-the-countrys-financial-services-sector-395368-2023-08-24, (visited on October 15, 2023).

number of restrictions has skyrocketed in the last several years. Smaller banks are also required to comply with regulatory requirements, just like large banks.[86]

**4.2.3 Data Protection:** Data gathered from reports reveals that over 60% of clients are ignorant of the information regarding cyber security risks associated with banking operations. Furthermore, about 55% of customers are not competent enough to exercise extra caution when using online banking services.[87] Due to the substantial volume of Personally Identifiable Information (PII) and financial data they manage, banks are prime targets for hackers. To meet the growing demand for cost-effective services, many banks are adopting cloud and IoT solutions for data transfers and transactions. Recognizing the importance of data privacy, along with regulatory concerns, banks prioritize data security and efficient management. However, the presence of outdated on-premise legacy systems, intertwined with various custom applications, poses challenges. While legacy systems are essential for critical services, they struggle to keep pace with the demands of modern banking, leading to increased security risks.[88] Along with the security the unawareness of the customers towards developing cybercrimes poses a great threat for the Indian Banking sector in protection sensitive information.

**4.2.4 Lack of Cyber literacy in the Board of Directors:** An Independent Director serves as a mentor and advisor to the company, enhancing corporate credibility and governance. They act as a watchdog, aiding in risk management and improving governance standards. Independent directors actively participate in company committees to ensure better governance. In a study undertaken by the national stock exchange and the Institutional Investory Advisory Services and covering companies of Nifty 50 and Nifty Midcap 50 indices, it was found that only 58 out of 100 companies have independent directors with domain knowledge. Only 56 companies have technological and cybersecurity skills on their board even though cybersecurity is a growing business risk due to data breaches, failed regulatory compliances or lost trade secrets.[89]

---

[86] "*The 7 Top Cyber security Challenges for Financial Institutions*", https://cyberone.security/7-cybersecurity-challenges-facing-financial-institutions-and-how-to-overcome-them/, (visited on October 7, 2023).
[87] Supra Note 81.
[88] Neelam Sethi, "*Cyber Security analysis in Banking Sector*", INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMMERCE, MANAGEMENT & SOCIAL SCIENCE, Vol 04, No. 03(I), July - September, 2021, pp. 63.
[89] Kiran Kabtta Somvanshi, "*India Inc needs independent directors with domain knowledge, directors with cyber security skills: NSE study*", Economic Times, June 18, 2021, https://economictimes.indiatimes.com/markets/stocks/news/nse-study-finds-india-inc-needing-independent-directors-with-domain-knowledge-and-directors-with-cyber-security-skills/articleshow/83625692.cms, (visited on October 15, 2023).

This shows a lack of responsibility on the part of the banks as they should have such members on board that have domain knowledge or get trained in these matters.

**4.2.5. Complexity-** Organizations providing financial services have extremely sophisticated IT infrastructure that combines both established and cutting-edge technologies. In addition to being risky, it is necessary to guarantee a robust and up-to-date consumer experience because complicated technological stacks are more likely to have security flaws and vulnerabilities. The most recent cyber threats, such as web attacks and next-generation ransomware, are being brought about by technological advancements. The necessity to improve cybersecurity is once again in the spotlight due to the rapid expansion of digital payment platforms in India and the country's move toward a cashless economy.[90] Banks are accountable for ensuring robust cybersecurity measures are there and are continuously updated. Lastly banks have the responsibility to implement best practices in cybersecurity and invest in technologies that protect data. Uninformed consumers are susceptible to deception due to a lack of understanding of the latest attack methodologies and identified preventive measures. Moreover, traditional law enforcement policies, standards, and methods have proven insufficient to address the evolving landscape of cybercrimes, leading to recurring criticisms of the effectiveness of the Information Technology Act in India.[91]

**4.2.6. The Growing threat of AI:** As Indian banks increasingly integrate AI to improve efficiency and customer experience, fraudsters are simultaneously exploiting the same technology to commit sophisticated scams. Deepfake-based fraud has become one of the fastest-growing threats in the country's financial sector, with a **550% rise since 2019** and projected losses estimated at **₹70,000 crore in 2024**, according to Pi-Labs. These scams go far beyond simple phishing, fraudsters now use AI-generated audio and video to impersonate real people with disturbing accuracy, enabling crimes such as identity theft, loan fraud, and fake insurance claims. A **McAfee survey** revealed that over **75% of Indians** have come across deepfake content in the past year, and nearly **38%** have fallen victim to scams involving manipulated media. The increasing sophistication of AI-generated deception makes distinguishing real from fake not just difficult, but critical for banks whose credibility depends on trust and security. One of the most vulnerable stages in banking operations is the **customer onboarding process**, where fraudsters use deepfake technology to bypass Know Your

[90] Ibid.
[91] Supra Note 6 p. 553.

Customer (KYC) checks. To counter this, banks are adopting **AI-driven video KYC systems** capable of detecting manipulation indicators. However, the threat extends beyond onboarding. Cybercriminals have begun using **voice cloning and deepfake videos** to impersonate senior executives and trick employees into authorizing fake transactions. Traditional safeguards like **passwords and OTPs** are proving increasingly inadequate against these AI-powered scams. Ultimately, deepfake fraud represents a new frontier of cybercrime that blurs the line between authenticity and deception.[92]

### 4.3 Way forward

The management of a company under its corporate governance must also include cyber risk management too, as cybersecurity is an integral part of the overall management and impacts its governance. Cybersecurity is method through which these cybercrime can be fought against. The board and senior management must prioritize cybersecurity awareness and governance. Regular board discussions, inclusion of cybersecurity executives, and engagement with external experts are crucial. The board should guide the management team in fostering a strong cyber risk management culture. Audit committees should focus on risk-driven audits and self-assessments, while risk committees must review cyber risk strategies and disaster recovery plans. The senior management team should implement policies, ensure effective communication channels, and prioritize staff training for cyber risk management. Overall, a collaborative and proactive approach is vital for comprehensive cyber risk governance.[93]

## CONCLUSION AND SUGGESTIONS

### 5.1 Conclusion

Indian Banking sector is a major source of economic growth, but is also a prime target for the cybercriminals because of the country's rapid digitalization in the banking environment. The Indian banking industry needs to have strong cybersecurity and resilience architecture that is continuously updated as per the advancements in the technologies, as cyber threats are constantly evolving. From the critical analysis done it was observed that the growing

[92]Ankit Ratan, "*The sudoku of fraud detection: How banks can use AI to spot AI-generated deepfakes*", The Economic Times, May 24, 2025, CISO, https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/ai-vs-ai-protecting-banks-from-the-rising-tide-of-deepfake-fraud-in-india/121368083, (visited on September 15, 2025).

[93] "*Redefining Corporate Governance for Better Cyberrisk Management*", https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-4/redefining-corporate-governance-for-better-cyberrisk-management_joa_eng_0719, (visited on September 15, 2025).

preference for online services among Indian consumers, driven by the allure of convenience and cost-effectiveness, has led to a surge in online transactions. However, this trend has also exposed vulnerabilities in cybersecurity measures implemented by financial institutions. Despite efforts to promote cashless transactions, the rapidly evolving technological landscape and the increasing expertise of cyber intruders pose significant challenges.

Cybercrime, with its unique and attractive features such as anonymity, global reach, and swift results, has begun to overshadow traditional crimes. The lack of awareness campaigns further exacerbates the situation, making uninformed consumers easy targets for cybercriminals who exploit their limited understanding of the latest attack methodologies and preventive measures.

The battle against AI-driven fraud has become a relentless race between cybercriminals and financial institutions. As deepfake scams grow more sophisticated, banks must strengthen their defenses through advanced tools such as video-based KYC, behavioral analytics, and real-time fraud detection systems. Detecting these crimes now resembles solving a high-stakes puzzle demanding precision, vigilance, and smart strategy. By constantly upgrading their security frameworks, banks can protect customers, secure financial assets, and reinforce public trust in India's digital banking network. Those that take proactive steps today will not only reduce risks but also emerge as leaders in financial security, setting new standards in a rapidly evolving digital landscape.

Significant steps have been taken by the Reserve Bank of India (RBI) to address the cybersecurity challenges, which includes issuing comprehensive guidelines and standards such as the Cyber Security Framework for Banks. Mandating adherence to ISO/IEC 27001 and 27002 standards, the RBI has set a strong foundation for cybersecurity preparedness. Additionally, the introduction of the Digital Personal Data Protection Act of 2023 provides a modern legal framework to safeguard individuals' data, ensuring greater accountability and stringent measures against data breaches. However, the effectiveness of these regulations depends not just on their implementation but also on the active cooperation and continuous vigilance of financial institutions. With penalties imposed for non-compliance and breaches, the financial sector is under substantial pressure to bolster its cybersecurity posture. Thus the hypothesis that the rapid digital transformation of the Indian banking sector, designed to enhance customer accessibility and convenience, simultaneously exposes opportunities for cybercriminals to exploit digital infrastructure vulnerabilities, posing challenges in the

effective implementation of cybersecurity mechanisms by banks, stands proved.

### 5.2 Suggestions

After critically analysing the issue the researcher observed that to address the issues and challenges observed in this area, certain suggestions can help the Indian Banking sector to enhance its cybersecurity and corporate governance

- India needs to sign the Convention on Cybercrime 2001, to facilitate the extradition of criminals or sign mutual assistance treaties with other countries, next would be to have a unified law which will lessen the burden of the banks and they would be able to adequately comply with the provisions.

- Guidelines that are being issued by different regulators are contradictory to each other, the solution to this is to clear what are specified purpose for which data of any customer can be accessed or removed. What should be the extent to which the data can be accessed, as banks need the access to the accounts of the customers to provide them protection from cyber threats.

- The Banking institutions need to proactively educate their stakeholders of the cybersecurity risks associated with the banking operations. The awareness programmes should focus on raising awareness about the potential threats, the importance of data protection, and measures by which they can enhance their online security. By doing this bank empower clients to make informed decisions, exercise caution, and build confidence and trust among stakeholders.

- The banks should appoint such members only those who have domain knowledge or have the members trained in emerging areas, make its stakeholders aware of the latest cyber threats and attacks. The board and senior management need to make cybersecurity awareness and governance a top priority. It is essential to have frequent board discussions, involve cybersecurity executives, and seek input from external experts. The board's role includes guiding the management team in cultivating a robust culture of managing cyber risks effectively.

- If the banks use machine learning-powered cybersecurity tools that keep track of

customers' spending patterns and help detect when any account has been compromised, it helps to handle the situation before the damage becomes serious. Another tool that could be used is the Data Loss Prevention tools, which keep data safe, prevent it from leaks and reach compliance with different data privacy laws. Further use of network insight products can provide the banks with a centralized view of their network data to identify vulnerabilities and loopholes in advance.

- Tackling AI-driven cybercrime requires a comprehensive and adaptive strategy that blends legal reform, technology, and awareness. As deepfakes and algorithmic manipulation grow more sophisticated, cyber laws must be regularly updated to address new risks, while ethical frameworks should ensure that AI use in law enforcement respects human rights and avoids bias. Law enforcement agencies need specialized training to understand and manage AI-based threats effectively. Banks must deploy AI-powered security tools such as biometric verification, behavioral analytics, and deepfake detection systems that can identify anomalies in real time during onboarding and transactions. Employee training on emerging digital fraud methods and the adoption of multi-layer authentication systems like voice biometrics and behavioral monitoring can further enhance protection. Collaboration with research institutions and cybersecurity firms will help develop adaptive fraud detection models that evolve with changing attack patterns. Simultaneously, public awareness campaigns are vital to educate users about AI-generated scams, empowering them to safeguard their digital identities.

- Different banks and organizations can share their cyberattack experiences, and how they overcame it, this can help other organisations to be prepared beforehand.

Since prevention is better than cure which is particularly true for cybersecurity in banks. So, if banks invest in cybersecurity it will not help improve their corporate governance but also will be an important step in staying competitive and future ready.

## BIBLIOGRAPHY

### I. Printed Sources

#### 1. Books


- Prof. R.K. Chaubey, AN INTRODUCTION TO CYBER CRIME AND CYBER LAW, 2nd ed. 2012, Kamal Law House.

- Vakul Sharma, INFORMATION TECHNOLOGY LAW AND PRACTICE, 5th ed. 2017, Universal Law Publishing.


#### 2. Articles: -


- Manasi Sutar and Mayuri Talegaonkar, Review of Cyber Security Threat in Banking Sector during Covid-19 Pandemic, "INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY", Volume 2, June 2022.

- Simran Singhi and Vaishnavee Upreti "Corporate Governance and Cyber Security", INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES, Vol.4, 2021.

- Seema Goel, "Cyber-crime: A Growing threat to Indian Banking Sector", International Journal of Science and Technology Management, Vol 5, 2016.

- Neelam Sethi, "Cyber Security analysis in Banking Sector" INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMMERCE, MANAGEMENT & SOCIAL SCIENCE, Vol 04, July - September, 2021.

- Madhura Pitre, "Critical analysis of legal framework regulating internet banking in India" INDIAN JOURNAL OF INTEGRATED RESEARCH IN LAW, Vol 3, 2023.

- Nuruddin Khan, Dr. Shobha Gulati, "International Legislative Framework of Cybercrimes- A Comparative Study of India, Israel, And USA", JOURNAL OF POSITIVE SCHOOL PSYCHOLOGY, Vol. 7, 2023.

- Neeta and V.K. Bakshi, "Cyber Crimes In Banking Sector", AAYUSHI INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL, Vol 4, May 2019, P 25-31.


## II. Electronic Sources

### 1. Webliography: -


- https://www.knowledgehut.com/blog/security/cyber-security-in-banking
- https://cyberone.security/7-cybersecurity-challenges-facing-financial-institutions-and-how-to-overcome-them/
- https://www.firstpost.com/opinion-news-expert-views-news-analysis-firstpost-viewpoint/indian-banking-sector-at-forefront-of-cyber-attacks-what-are-major-threats-and-way-ahead-11620701.html
- https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-changing-role-of-the-board-on-cybersecurity-noexp.pdf
- https://www.azbpartners.com/bank/cybersecurity-2021-india-chapter/
- https://www.moneycontrol.com/news/business/rbi-imposes-rs-5-39-cr-penalty-on-paytm-payments-bank-for-kyc-norms-violation-11522081.html
- https://www.medianama.com/2017/10/223-rbi-fines-yes-bank-failing-report-cyber-security-attack-atm-network/
- http://timesofindia.indiatimes.com/articleshow/101425742.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10999
- https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0
- https://www.upguard.com/blog/cybersecurity-regulations-india

- https://www.knowledgehut.com/blog/security/cyber-security-in-banking
- https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks
- https://download.manageengine.com/images/indian-banking-industry-39s-cybersecuritywhitepaper.pdf?pos=BFSI
- https://sbi.co.in/web/personalbanking/cybersecurity#:~:text=To%20report%20any%20cyber%20incident,cyber%20crime%20helpline%20number%201930.
- SYSTEMhttps://primelegal.in/2023/06/11/significance-of-cybersecurity-in-indianbankingsystem/#:~:text=Banking%20cybersecurity%20solutions%20include%20network,frequent%20security%20evaluations%20and%20testing.
- https://download.manageengine.com/products/desktop-central/indian-banking-whitepaper.pdf
- https://www.sebi.gov.in/legal/regulations/nov-2021/securities-and-exchange-board-of-india-listing-obligations-and-disclosure-requirements-regulations-2015-last-amended-on-november-09-2021-_37269.html
- https://www.icslearn.co.uk/blog/corporate-governance/4-consequences-of-poor-corporate-governance
- https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security
- https://delhidistrictcourts.nic.in/ejournals/CYBER%20LAW.pdf
- https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
- https://www.sebi.gov.in/legal/circulars/jan-2020/non-compliance-with-certain-provisions-of-the-sebi-listing-obligations-and-disclosure-requirements-regulations-2015-and-the-standard-operating-procedure-for-suspension-and-revocation-of-trading-of-_45752.html
- https://www.sebi.gov.in/legal/regulations/nov-2021/securities-and-exchange-board-of-

india-listing-obligations-and-disclosure-requirements-regulations-2015-last-amended-on-november-09-2021-_37269.html

- https://www.businesstoday.in/opinion/columns/story/indias-new-data-protection-law-heres-how-the-landmark-law-can-impact-the-countrys-financial-services-sector-395368-2023-08-24