LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 2 | Issue 3

2024

CYBER SECURITY MENACES IN BANKING: EMERGING PERILS AND WAYS TO MITIGATION

Swesthiga K[1]

I. ABSTRACT

As the backbone in current economies, the banking sector has experienced a digital revolution, utilising technology to improve client satisfaction, accessibility, and efficiency. But this higher dependence on the internet has also made the banking industry more vulnerable to a complicated and dynamic threat environment. Cyber-attacks are becoming a constant and serious problem for financial institutions around the globe. They can take many different forms, from clever phishing operations to advanced continuing dangers. Persistent cyber-attacks have profound consequences on banks, including monetary losses, harm to their company, a decline in customer trust, and possible systemic dangers to the overall economy. The banking sector must proactively modify its cyber security defences to keep ahead of new threats as scammers' strategies get more complex. In order to improve banking security, this study intends to discover new cyber security threats in the banking industry, analyse their potential effects on the banking sector, and assess successful mitigation methods.

The author will examine upcoming dangers and trends in addition to existing threats, weaknesses, and security precautions. Out-dated systems, limited personnel training, and inadequate incident response strategies are some of the main hazards. Establishing strong security frameworks, carrying out routine risk assessments, and utilising AI-powered threat detection are examples of effective mitigation techniques. This study advances knowledge about new cyber security risks in the banking industry and offers practical suggestions for financial entities looking to strengthen their safety measures. Banks can safeguard consumer information, stop financial losses, and uphold confidence in the financial system by addressing these new dangers.

[1] Masters in Law Graduate - The National University of Advanced Legal Studies.

II. KEYWORDS

Cyber-security, banking, hazardous, cyber-criminals and mitigation.

III. INTRODUCTION

Cyber security safeguards a person's phone, computer and other online information from hacking, malware, phishing, virus and hazardous activities. Same way, cyber security in banking protects the customer's bank account, transaction and data from fraudulent activities. With the emergence of digital technology, the banking sector, which was once a stronghold of traditional transactions and physical security, has experienced a radical transformation. Cyber security threats are a new set of difficulties that have emerged alongside the extraordinary comfort and efficiency brought about by this revolution. Cybercriminals view the banking industry as a prime target because of the complex network of digital banking systems and the enormous value of financial information.

The world of cyber threats has changed drastically in the last several years, with hackers growing more deceitful and determined in their efforts for financial gain. Cyber security menaces causes significant risks to the banking industry and mitigation strategies are important to protect against emerging perils. The paper delves into the understanding of cyber security risks in banking, how these cyber-attacks affects the banking sector, how technologies play a role in cyber security and what are the ways to mitigate the cyber threats.

IV. EXPLORATION OF CYBERSECURITY MENACES IN BANKING

The widespread adoption of digital transactions, along with the vast systems containing confidential financial information, has made banks incredibly appealing targets for hackers. These criminals use a constantly changing toolkit of techniques to break into networks, steal money, and interfere with operations. These strategies range from advanced ransom ware attacks to phishing schemes and malware. A financial institution that experiences a successful cyber-attack might have disastrous effects on its clients, the economy as a whole, and the bank itself. Understanding the

complicated details that define these risks is vital in order to formulate efficacious remedial strategies and preserve the security of the entire financial system. The following are different types of cyber security menaces that arise in banking:[2]

Phishing - In phishing, fraudsters use fake emails, messages or websites to trick the bank customers to make them reveal sensitive banking details like passwords, credit card details and other personal data. For example, imagine a mail from the State Bank of India (SBI) stating that "Your bank account will be removed or deactivated if you do not re-set your password". Here, the bank customer will be tricked and they will do that action and thereby personal information will be shared to the fraudster. Phishing in banking can happen through any mode other than emails which include phone calls, bank websites which are fraudulent, etc.

Malware - Malware in banking basically is maleficent software which is created to affect or ruin banking related information of the user. Through this action, fraudsters take sensitive bank details, distort banking services in online, create hidden starting points for future hacking attempts, etc. Malware may occur through phishing, software downloads which are weak, improper pen drives, etc.

Ransom ware - In the banking industry, ransom ware is a term used to describe a kind of malicious software that hides and locks down access to the data, systems, or customer information of banks or other financial institutions, then demands a ransom to be paid in exchange for a key to unlock it. Ransom ware may affect the banking system through phishing or other fraudulent activities which will affect the bank customer like financial loss, breach of data, system error, etc. There are also other way to hack which includes malicious spam and malicious advertising.

Distributed denial-of-service (DDoS) - DDoS attacks are cyber-attacks in which a bank's internet sites are overloaded with traffic from numerous hacked devices or systems, leaving them inaccessible to verified users.[3] Here, hackers have global control over several software programs. The online resources of the bank receive traffic from

[2] Dorota Jasińska and Marcin Dobosz, 'Cybersecurity in Banking: Threats and Mitigation Strategies' (2024) Neontri <https://neontri.com/blog/cybersecurity-in-banking/> accessed 22 August 2024

[3] 'What is a DDoS attack?' <https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/> accessed 22 August 2024

these computer programs continuously. Overloaded systems at the bank start to lag or even crash. Then this will make the customers who are trustworthy, unable to access their accounts or make purchases.

Third-Party Risk and Remote Workforce - Third-Party Risk in banking means the possible dangers and weaknesses that might occur when a bank collaborates with or contracts with outside vendors, contractors, or third-party providers. Remote workforce in banking means the program that permits staff members to work remotely or from home rather than in a traditional office setting and this will cause problems like cyber security perils, data privacy issues, etc.

Mobile Vulnerabilities - Nowadays, people cannot live with mobile and it became a very important possession for them. Mobile vulnerabilities in banking means security issues in banking apps of platforms in mobile that are caused by the fraudsters to obtain sensitive bank details, steal money and disrupt services. This activity will also happen when a mobile is lost or stolen.

V. THE IMPACT OF CYBERATTACKS ON THE BANKING SECTOR

The possibility of digital attacks is growing as the banking sector goes more online, affecting sensitive customer information and the safety of the financial system. According to the Reserve Bank of India's (RBI) Financial Stability Report, the banking sector recorded more than 20,000 cyber-attacks in the last 20 years, resulting in $20 billion in losses. Following a report by the Data Security Council of India, in December 2023, surfing on malicious links in emails and websites is responsible for 25% of these threats in India. Scheduled Commercial Banks (SCBs) reported 69% of cyber-attacks on financial institutions, followed by Urban Co-operative Banks (19%) and Non-Banking Finance Companies (NBFCs) with 12%.[4] The following talks about how cyber-attacks impact the banking sector.

[4] Abhyjith K. Ashokan, 'RBI warns banks of cyberattacks, scheduled commercial banks at highest risk' *Hindustan Times* (India, 29 June 2024) <https://www.hindustantimes.com/business/rbi-warns-banks-of-cyberattacks-scheduled-commercial-banks-at-highest-risk-101719637827991.html> accessed 23 August 2024

Based on Eurofins data and the authors' own observations, employee-targeted phishing has surged since the pandemic as a result of the growing popularity of remote work and the additional workload that the pandemic has either directly or indirectly created[5]. As per Verizon's review, thirty per cent of the malware was installed manually by hackers, twenty per cent was downloaded from an application, and twenty-three per cent of the malware being spread was sent by email. The most significant shift is the rise of corrosive attacks.

The purpose of the attacks is not to steal money, but rather to corrupt files or data on particular systems in order to disrupt networks or services. Destructive attacks impacted 25% of the financial institutions surveyed in 2020. Cyber experts highlight that regrettably, the issue that financial institutions now need to answer is "when" rather than "if" they are going to be attacked.[6]

Now let us look into how the above-mentioned cyber security attacks impacts the banking sector. Phishing in banking is vicious as the fraudsters may steal bank customer's money, bank account or may even send their bank details to the dark web. Malware problems have been known to seriously affect banking services by harming the security of payments and client information. Malware has a tendency to attack banking systems and frameworks, resulting in major disruptions, losses in money, and loss to the institution's image. Banks are especially prone to ransom ware attacks, which lock important data and demand large ransoms to unlock the key. Rapid development of ransom ware may damage system operations, banking details, and customer information. If a bank follows the attacker's demands, it might be forced to pay a large amount in addition to taking legal and regulatory punishments for doing so.

DDoS can result in financial losses, decreased productivity, upset clients, and opportunity for attackers to conduct additional breaches. Hacking, system attacks, and interruptions to crucial services are examples of third-party risks. In addition to

[5] Olivér Gulyás and Gábor Kiss, 'Impact of cyber-attacks on the financial institutions' (2022) Elsevier B.V <https://pdf.sciencedirectassets.com/280203/1-s2.0-S1877050923X00039/1-s2.0-S1877050923002752/main.pdf> accessed 24 August 2024

[6] ibid.

creating additional dangers and vulnerabilities, remote work can further confuse the distinction between personal and professional gadgets. Attackers may be able to obtain private information, breach accounts, or interfere with mobile banking services through mobile vulnerabilities.

VI. TECHNOLOGY'S ROLE IN STRENGTHENING CYBERSECURITY

Technology is vital to cyber security because it is the primary source of protection against online attacks in banking. Actual surveillance, crisis management, and predictive analytics are made possible by cutting-edge technologies like automation, Machine Learning (ML), and artificial intelligence (AI). Networks and data are safeguarded by Intrusion Detection Systems (IDS), firewalls, and encryption. Furthermore, biometrics and block chain technology improve security measures, and virtualization and cloud security offer adaptable and expandable security. Banking sectors may improve their cyber security positions, lower risks, and keep ahead of new threats by utilizing these technologies.

Let us now look into how technology plays an important role in cyber security.[7] Block chain technology is now recognised as a means that businesses may secure their data, as the volume of data stored online and in the cloud approaches exceedingly large levels. By offering a safe, organised, and accessible method of conducting transactions, storing data, and verifying individuals, block chain technology improves cyber security in banking by lowering the risk of deception and cyber-attacks. Now days, AI is developing and used from schools to workplace as the world is becoming more digital.

AI has an enormous effect on banking's cyber security by allowing banks to quickly find new dangers and detect and mitigate threats in seconds by identifying developments, defects, and loopholes. Also, In order to evaluate banking's online

[7] Mira Ray, 'The Role of Technology in Cybersecurity' (*Innovators Central,* 22 June 2022) <https://innovatorscentral.ca/technology-in-cybersecurity/> accessed 25 August 2024

safety and create new security procedures and enhancements, advanced analytics engines can navigate through data and use analysis of patterns.

VII. FORTIFYING AGAINST THREATS: MITIGATION AND RECOVERY

Firm cyber security protocols provide protection against ransom ware, data breaches, and other criminal acts. Image protection, customer trust, and business continuity are all maintained by a strong preventive and recovery plan. Banks may actively combat emerging threats and promote a safe banking atmosphere by placing a significant emphasis on cyber security.

VIII. RELEVANT LAWS AND REGULATIONS:

The following are the legal and regulatory frameworks for cyber security threats in banking:[8]

A. The Information Technology (IT) Act, 2000:[9]

This is the basis of India's cyber laws, which offer a framework for cybercrime, e-commerce, e-governance, and data protection. It describes various cyber-crimes including theft of information, hacking, and online fraud.

Section 43A of the IT Act talks about "*compensation for failure to protect data*".[10] It says that an organization, which also includes banking sector, to safeguard sensitive personal information like financial information which they collect from the customers, to take security measures to prevent cyber-attacks and nurturing cyber security practices and procedures which should be in line with the rules and regulations.[11]

Section 72A of the IT Act talks about "*Punishment for disclosure of information in breach of lawful contract*".[12] It says that if a person has access to personal information because of his/her job or lawful contract and they share or send this details to others without

[8] Kyle Chin, 'Top Cybersecurity Regulations in India [Updated 2024]' (*UpGuard,* 18 January 2024) <https://www.upguard.com/blog/cybersecurity-regulations-india> accessed 25 August 2024
[9] The Information Technology Act, 2000 (Act 21 of 2000).
[10] The Information Technology Act 2000, s 43A
[11] ibid.
[12] The Information Technology Act 2000, s 72A

consent or by hacking, that person will be punished with imprisonment for a term of three years and/or a fine of Rs. 5,00,000.[13]

B. The Information Technology (Amendment) Act, 2008:[14]

The IT Act was significantly expanded by the IT Amendment Act, which was passed in October 2008 and went into effect the following year. The initial measure, which had not opened the door for more advancement in IT, was improved by these modifications. It was welcomed as an interesting and highly expected step towards India's strengthened cyber security structure.

The IT Amendment Act has included the expanded definition of cybercrime then the punishments have also been increased when compared to the 2000 Act. Interestingly, the Amendment Act requires the reporting of data infringement to the authorities and it also inspires banking sectors to create a comprehensive cyber security framework. In a nutshell, this Act includes important features including strict legal frameworks, encouraging strong security frameworks, creating strong cooperation between banks and authorities for the protection of the information of the bank users.

We also have the Information Technology Rules, 2011.[15] The IT Rules is also known as Privacy Rules. The Rules was made in reference with some sections under the IT Act. The measures regarding operator regulation, updated fines and penalties for cybercrime, cheating, slanders, and unlawful publishing of private photos as well as speech constraints and censorship, are among the most important changes. The collecting of private data and other sensitive information, data protection, data retention, and processing of sensitive information by Indian companies and organisations are all governed by the IT Rules. Other Indian companies with separate legislation that address data privacy include banking, insurance, telecom, and healthcare.

[13] ibid.
[14] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009).
[15] The Information Technology (Reasonable Security Practices And Procedures And Sensitive Personal Data Or Information) Rules, 2011

Let us now look into the recent IT Rules that is, the Information Technology Rules, 2021.[16] The Ministry of Electronics and Information Technology replaced the IT Rules, 2011 with the IT Rules, 2021 on February 25, 2021. The Ministry released the updated draft modifications to the IT Act on June 6, 2022, just over a year after. These changes aim to make the Act better and more responsive to the demands of the rapidly evolving digital environment. The proposed changes intend to provide further surveillance on organisations (including banks) and give regular users of digital platforms the power to demand action when their rights are violated and seek compensation for their claims.

C. National Cyber Security Policy, 2013:

The National Cyber Security Policy 2013 was issued in 2013 by the Department of Electronics and Information Technology as a framework for security to help public and private organisations strengthen themselves against cybercrime. The Policy seeks to advance safety of India's cyber ecosystem by establishing more dynamic regulations. Through skill development and training, the policy hopes to produce over 500,000 skilled IT professionals over the next five years.

D. The National Cyber Security Strategy 2020:

The goal of this strategy is to raise the standard of cyber security reviews so that companies can perform more thorough assessments of their cyber security expertise and design. It is hoped that after the policy is put into effect, cyber examiners will raise the requirements on security, which would motivate companies to strengthen their security measures.

Know Your Customer (KYC):

KYC procedures are required by the RBI and norms and practices are utilised globally. KYC is the process of tracking and monitoring the security of customer data to better protect against fraud and the theft of payment credentials. Financial institutions such as banks, insurance providers, and other online transaction firms must ensure that

[16] The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021

every one of their users can be trusted and verified.[17] It's essential to note that banks, companies, and businesses who violate the KYC guidelines risk a financial penalty of Rs. 2 lakh.

E. The Digital Personal Data Protection (DPDP) Act, 2023:[18]

The DPDP was passed by the Indian Central Government in August 11, 2023. The European Union's (EU) General Data Protection Regulation (GDPR) provides a comprehensive definition of personal data, which the act adopts in order to safeguard data principals and limit the actions of data trustees. Furthermore, the DPDP identified an entirely different category of data fiduciaries and instituted the Data Protection Board of India. Organisations classified as important information trustees by the government are deemed at greater threat. Organisations that are found to be essential information trustees are subject to further regulations.

There are also some regulatory bodies that protect cyber security in banking against perils like Computer Emergency Response Team (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), Cyber Regulations Appellate Tribunal (CRAT), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority (IRDAI), Telecom Regulatory Authority of India (TRAI) and Department of Telecommunications (DoT).[19]

MITIGATION STEPS:

Cybercriminals target banking services a lot, exposing personal client information and finances at serious danger. Robust mitigation measures are essential to combat these hazards. Banks can fortify the walls and protect their digital possessions by implementing the measures.

---

[17] 'Master Direction - Know Your Customer (KYC) Direction, 2016' (*RBI*, 29 May 2019) <https://www.rbi.org.in/CommonPerson/english/scripts/notification.aspx?id=2607#:~:text=%E2%80%9CDigital%20KYC%E2%80%9D%20means%20the%20capturing,the%20RE%20as%20per%20the> accessed 26 January 2024

[18]The Digital Personal Data Protection Act, 2023 (Act 22 of 2023)

[19] Kyle Chin, 'Top Cybersecurity Regulations in India [Updated 2024]' (*UpGuard,* 18 January 2024) <https://www.upguard.com/blog/cybersecurity-regulations-india> accessed 26 August 2024

Enhancing the security of data and financial assets can be achieved by combining cyber security techniques with essential business processes like finance. This coordinated strategy effectively lowers cyber dangers. Companies should have the flexibility to quickly adapt their cyber security plans in response to emerging threats. To keep ahead of cyber enemies, it requires for a constant dedication to education and creativity. The requirement to concentrate funds on cyber security projects that result in a major reduction in risks. Organisations must focus on working in the areas that will have the biggest benefits.[20]

There are also other important ways to mitigate cyber security threats in banking. They are as follows:[21]

Banks need to be vigilant about monitoring the internet for any abuse of product names, brand names, logos, and other trademarks. This approach aims to cover everything, from phishing sites and lookalike domains to false applications and fictitious social network profiles. Threat intelligence reveals malware logs from the deep and dark web and illuminates the most recent strategies and methods used by threat actors to create and distribute malware, enabling banks and other financial institutions to identify stolen information and take preventative measures.

As the scope of attacks grows and changes, simplifying the process of finding and listing external assets will save time and enable the detection of new assets. Banks should also keep an eye out for data leaks on the dark web. Early detection of this danger by the security team will allow them to force vulnerable users to update their passwords before any accounts are hacked. Also worth mentioning, employees in the banking industry can greatly enhance their personal security protocols with the use of security awareness training.

---

[20] Adedoyin Tolulope and three others, 'Cybersecurity risks in online banking: A detailed review and preventive strategies application' (2024) WJARR < https://www.researchgate.net/profile/Adedoyin-Oyewole-2/publication/379428581_Cybersecurity_risks_in_online_banking_A_detailed_review_and_preventive_strategies_applicatio/links/6611a4ac2034097c54fb755f/Cybersecurity-risks-in-online-banking-A-detailed-review-and-preventive-strategies-applicatio.pdf > accessed 26 August 2024

[21] Daniel Pigeon, 'Top 5 Cyber Risk Mitigation Strategies For The Finance Industry' (*Cyberint*, 14 March 2023) < https://cyberint.com/blog/financial-services/right-on-the-money-cyber-risk-mitigation-strategies-for-the-finance-industry/> accessed 27 August 2024

IX. CONCLUSION

Cyber security threats are on the rise in banks, creating significant risks to data integrity, trust among clients, and financial stability. The paper found the alarming range of cyber-attacks, ranging from advanced nation-state threats to ransom ware and phishing schemes. As we've seen, such attacks can have disastrous effects, exposing private data, interfering with company functions, and weakening customer trust. The research paper has also shown how important technology is to boosting cyber security from AI-powered emergency response to effective identifying a threat.

In a nutshell, banks need to take a variety of steps to protect themselves against these dangers, incorporating proactive strategies for recovery, strong mitigation techniques, and on-going training for staff. The safeguards currently in place for the banking system must also change as a hazardous circumstance does. Banks may safeguard the integrity of the financial system, their reputation, and their clients by understanding the seriousness of these cyber security threats and taking proactive steps to mitigate them. The future of banking is at the forefront, so this is the time to take action.

X. BIBLIOGRAPHY

1. Abhyjith K. Ashokan, 'RBI warns banks of cyberattacks, scheduled commercial banks at highest risk' *Hindustan Times,* 29 June 2024.
2. Adedoyin Tolulope and three others, 'Cybersecurity risks in online banking: A detailed review and preventive strategies application' WJARR, 2024.
3. Kyle Chin, 'Top Cybersecurity Regulations in India [Updated 2024]' *UpGuard,* 18 January 2024.
4. Dorota Jasińska and Marcin Dobosz, 'Cybersecurity in Banking: Threats and Mitigation Strategies' Neontri, 2024.
5. Daniel Pigeon, 'Top 5 Cyber Risk Mitigation Strategies For The Finance Industry' Cyberint, 14 March 2023.
6. Mira Ray, 'The Role of Technology in Cybersecurity' *Innovators Central,* 22 June 2022.
7. Olivér Gulyás and Gábor Kiss, 'Impact of cyber-attacks on the financial institutions' Elsevier B.V, 2022.