WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Analytical Study on Cybersecurity Threats in the Indian Banking Sector

Mrs. Shashikala K.G[1], Mr. Ramesh A.P[2]

[1] Assistant Professor Economics Department SDM College of Business Management Mangalore 575001
E-Mail: shashikala_kg@sdmcbm.ac.in
[2] Assistant Librarian UHS, Bagalkot
E-Mail: ramesh.ap@uhsbagalkot.edu.in
9844125902

ABSTRACT :

Cybersecurity has become as essential to modern life as the technology it aims to safeguard. The two are inextricably linked—our economic stability, national defense, and the very structure of our society now rely heavily on digital systems. Cybersecurity, therefore, plays a crucial role in maintaining national interest, economic prosperity, and public trust. The term "cyber" is a prefix that signifies a person, concept, or object associated with the computer and information age. Derived from the Greek word Kybernetes, meaning “steersman” or “governor,” it was popularized through the term “cybernetics,” coined by Norbert Wiener. The digital realm we navigate daily is known as cyberspace, and it is governed by a set of regulations referred to as cyber laws. These laws encompass all internet users, often termed “netizens,” and extend across national borders, establishing a form of universal jurisdiction. Cybercrime refers to criminal activities where a computer serves either as the primary target (such as in hacking, phishing, or spamming) or as a tool to facilitate other crimes (such as child pornography or hate-related offenses). Such crimes may involve the unauthorized extraction of personal data, theft of corporate secrets, or other exploitative or malicious uses of technology. The objective of this research paper is to examine the cybersecurity challenges confronting Indian banks in the digital era. Additionally, the study aims to analyse the general public’s level of awareness concerning cybercrimes and their implications, thereby highlighting the critical need for improved digital literacy and institutional safeguards.

Keywords: cyber security, banks, technology, challenges, cyber crimes

Introduction :

The ongoing COVID-19 pandemic has triggered a significant transformation across the globe, compelling countries to embrace digitalization at an accelerated pace. As societies become increasingly reliant on technology for essential services and daily operations, they simultaneously become more vulnerable to the inherent risks associated with it. While the digital revolution offers immense benefits, it also introduces complex security challenges. The growing dependence on technology has made it a prime target for cybercriminals, thereby placing cybersecurity at the center of national and institutional risk management strategies.Recognizing the urgency of the situation, the Reserve Bank of India (RBI) released the Technology Vision for Cyber Security for Urban Co-operative Banks (UCBs) – 2020–2023. This document, published on the RBI’s official website, is aimed at strengthening the cybersecurity framework of Urban Co-operative Banks to address the rapidly evolving threats in the information technology and cyber landscape. The goal is to enhance their resilience against a rising tide of cyber threats that continue to challenge banking operations. The year 2020, in particular, posed substantial cybersecurity challenges for Indian banks. The COVID-19 outbreak significantly disrupted banking operations, especially during the nationwide lockdowns. In response, banks quickly adapted by accelerating their digital initiatives, including the expansion of digital banking platforms and enabling remote access for employees. These measures ensured continuity of services and supported contactless banking, aligning with pandemic-related restrictions. However, this rapid digital shift also exposed the banking sector to a surge in cyber-attacks. Cybercriminals exploited new vulnerabilities created by remote work environments, increased digital transactions, and untested systems. As a result, Indian banks experienced a notable increase in financial frauds and data breaches. The expanding digital attack surface is expected to continue posing risks in the future.

These rising cyber threats have become a significant concern for both the banking sector and regulatory authorities, including the RBI. The situation underscores the need for a robust cybersecurity infrastructure capable of protecting computers, networks, software, and sensitive data from unauthorized access, malicious activity, and exploitation. As the digital ecosystem becomes more complex, the importance of information technology security in safeguarding financial institutions cannot be overstated.

Scope of the study

The banking sector is a critical pillar of India's economic growth, and since the late 1980s, Indian banks have actively implemented technological solutions to enhance efficiency and service delivery. However, this digital evolution has brought with it significant concerns regarding the protection of sensitive information and the privacy of data, exposing both institutions and customers to cybersecurity risks. Unlike many foreign banks, Indian banks operate on a much larger scale with vast networks and extensive human resources, making cybersecurity management particularly complex. Numerous international studies have stressed the importance of focused research on cybersecurity within the banking industry. In this context, the present study holds strong relevance, as it seeks to analyze and address the unique cybersecurity challenges faced by Indian banks in a rapidly evolving digital landscape, emphasizing the urgent need for effective and resilient risk management practices.

Literature Review

Arief R. et al. (2011) Group of Faculty of computer science from university of Indonesia specifically discusses about three types of applied ethics i.e. Cyber ethics, information ethics and computer ethics. There are two aspects of these three applied ethics that is there definitions and the issues associated with them. Authors also say that these three applied ethics acts as a base for e-government ethics and can enrich the e-governance of the country.

Ashwini B. (2012) Author discusses broadly about the ratio of increasing cyber crime and their effect on the society and e business and retailers. The paper briefs about the cyber threat and frauds, it also briefs about the internet user in India, its scope and future. Author also puts light on the governmental measures to stop cyber crime and talks about the challenges that India needs to face to beat cyber threat.

Bawa D. and Marwah D. (2011) Authors explain in this Cyber ethics refers to the code of responsible behaviour on the internet, this paper explores the codes of online conduct that are emerging as new media gains more influence in political and business affairs.

Brar et al. (2012) In their study on vulnerabilities in the security aspects of e- banking, observed that use of internet technologies have transformed banking industry from the customer and bank perspectives. The study further pointed out that it has greatly increased the number of criminal activities like customer identity theft, phishing, DoS attacks, malware attacks; ATM related cyber threats and credit card based cyber frauds.

Cezar V. (2012) This paper explores the notion of cyber attack as a concept for understanding modern conflicts. Author elaborates a conceptual theoretical framework, observing that when it comes to cyber attacks, cyber war and cyber defence there are no internationally accepted definitions on the subject.

National Cyber Security Policy Govt. Of India (2011) In this paper gives a detailed study about the cyber security, cyber space and its strategic perspective authors also explain that legal framework, law enforcement and information sharing. Paper also talks about the awareness created at different level of users (corporate, home users, students etc) through training. The paper is concluded by discussing the technologies used for ensuring security.

Sanjay P. (2010) Author discuss in detail the provisions of IT Act, 2000 and its recent amendments towards combating cyber crime. Author has also made an attempt to analyse the current trends in cyber crime then the analyses is made on the needs of legislation and current provisions of IT Act, lastly paper talks about similar provisions in the world and drawing parallel laws in the country. Finally author sums up the discussion with suggested recommendations for possible and safe cyber world.

Samridh S. et al. (2012) The paper proposes a curriculum for cyber safety education in schools. The proposed curriculum covers four sections: Cyber Threats, Protecting Ourselves, Cyber Ethics and Cyber Laws.

Objectives of the Research:

- To examine the attitude and awareness of people in India regarding the adoption of cyber security measures.
- To analyse the cyber security threats and challenges currently faced by Indian banks.
- To propose effective strategies and recommendations for addressing cyber security issues within the banking sector.

Research Methodology

This study primarily relies on secondary data collected from various sources such as websites, academic journals, and reference books. Additionally, primary data was gathered through a survey conducted with a sample of 50 respondents to assess the awareness levels of the general public regarding cybersecurity challenges.

Major Areas Covered in Cybersecurity

- *Application Security:* This involves implementing measures and countermeasures throughout the application development life cycle to safeguard applications from threats that may arise due to vulnerabilities in design, development, deployment, upgrades, or maintenance.
- *Information Security:* Information security focuses on protecting data from unauthorized access to prevent identity theft and maintain privacy. Key techniques include identification, authentication, and authorization of users to ensure that only legitimate individuals can access sensitive information.
- *Disaster Recovery:* Disaster recovery planning entails conducting risk assessments, prioritizing critical functions, and devising strategies to recover operations in the event of a disaster. It is essential for any business to have a solid disaster recovery plan to quickly restore normal operations following an unexpected disruption.
- *Network Security:* Network security involves activities aimed at protecting the usability, reliability, integrity, and safety of a network. Its goal is to detect, prevent, and stop a wide range of threats from entering or spreading across the network. Effective network security is essential for

safeguarding sensitive data and ensuring uninterrupted service. In recent years, India has experienced several unprecedented events that have brought cybersecurity concerns within the banking sector into sharp focus. A significant driving force behind this has been the Government of India's flagship Digital India initiative, which aims to transform the country into a digitally empowered society and knowledge economy. This initiative has accelerated the adoption of digital payments, with the value and volume of digital transactions reaching record highs, particularly in March 2017.

Additionally, the widespread penetration of inclusive banking under the Pradhan Mantri Jan Dhan Yojana (PMJDY)—which has led to over 29.18 crore accounts—has introduced many new users to formal banking services. However, this digital transformation has also exposed vulnerabilities. Notable incidents include the compromise of the SWIFT payment application in a major bank, resulting in large-scale fraudulent fund transfers, and a sophisticated attack on a payment processor that led to the large-scale compromise of debit cards across multiple banks.

As Nicholas Carr famously stated, "When a resource becomes essential to competition but inconsequential to strategy, the risks it creates become more important than the advantages it provides." In this context, cyber risk has become one of the most significant existential threats facing Indian banks today.

Technology Landscape

The digitization of financial transactions in India is accelerating rapidly. It is projected that non-cash payment transactions, which currently account for 22 percent of all consumer payments, will surpass cash transactions by the year 2023. The technological infrastructure supporting this growth is steadily expanding, with the country having over 100 crore mobile connections, including 24 crore smartphone users. By 2020, the number of smartphones increased to 52 crore, with approximately 90 percent of these devices being internet-enabled. Additionally, the number of internet users doubled from 300 million in 2015 to nearly 650 million by 2020.
Alongside this growth, Aadhaar enrolments are nearing saturation, with two states already reporting 100% coverage. The Pradhan Mantri Jan Dhan Yojana (PMJDY) has furthered the financial inclusion agenda, with almost 18 crore accounts opened in semi-urban and rural areas. It is important to recognize that a majority of these account holders are likely new to banking processes and the technological infrastructure that supports them, making them more vulnerable to social engineering tactics and other cyberattacks.

Cybersecurity Challenges

Several factors continue to influence the current state of cybersecurity in India:

- **Low Awareness:** Awareness among internal employees is crucial as they represent the first line of defense. However, many organizations do not invest adequately in training programs to raise cybersecurity awareness within their workforce.
- **Inadequate Budgets and Lack of Top Management Support:** Cybersecurity often receives low priority in budget allocations, which are typically driven by business demands. Top management support for cybersecurity initiatives also remains limited, largely due to a lack of understanding of the potential impacts of cyber threats.
- **Poor Identity and Access Management:** Identity and access management are fundamental to cybersecurity. In today's environment, where hackers often hold the upper hand, it only takes one compromised credential to gain unauthorized access to an enterprise network. Although some progress has been made, substantial improvements are still required in this area.
- **Ransomware on the Rise:** Recent malware attacks, such as WannaCry and Petya, have highlighted the growing threat posed by ransomware. As users become more aware of email-based ransomware risks, cybercriminals are exploring new attack vectors. Some are developing malware that can reinfect systems long after ransom payments, while others are using built-in tools and avoiding executable malware to evade endpoint protection systems. Moreover, ransomware authors are increasingly employing techniques beyond encryption, including deleting or corrupting file headers.
- **Mobile Devices and Apps:** With organizations increasingly adopting mobile devices as a primary channel for business operations, these devices have become prime targets for hackers. The ability to perform financial transactions through mobile apps has made smartphones attractive for attacks, leading to a rise in mobile malware. The use of jailbroken or rooted devices for financial activities further expands the risk surface.
- **Distributed Denial of Service (DDoS) Attacks:** The emergence of Internet of Things (IoT)-powered botnets has led to a surge in large-scale, destructive DDoS attacks. These attacks have intensified both in frequency and volume, necessitating improved response capabilities from organizations in India to mitigate such risks effectively.
- **Social Media:** The growing popularity of social media platforms presents increased opportunities for hackers to exploit user data. Many individuals share personal information publicly, which can be used to launch targeted attacks against their organizations. Furthermore, the use of social media to spread fake news can subtly damage the reputation of banks and other financial institutions.

Cybersecurity Initiatives in India

ISO 27001 (ISO27001) is the internationally recognized cybersecurity standard that provides a comprehensive framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and continuously improving an Information Security Management System (ISMS). This standard helps organizations systematically manage sensitive information and ensure its security.
India has developed a robust legal framework to address various aspects of cybersecurity, which includes the following key legislations:

- **Indian IT Act, 2000:** This act addresses numerous cyber offences with specific sections such as Section 65, which deals with tampering with computer source code; Section 66, which covers hacking and other computer-related offences; and Section 43, which relates to tampering of electronic records.
- **Indian Copyright Act:** This act makes it punishable for any person who knowingly uses an illegal copy of a computer program. While computer programs are protected under copyright law, they do not receive patent protection.
- **Indian Penal Code (IPC):** Relevant sections of the IPC include Section 406, which deals with punishment for criminal breach of trust, and Section 420, which addresses cheating and dishonestly inducing delivery of property.
- **Indian Contract Act, 1872:** This act provides legal remedies in case of breach of contract, including damages and specific performance of the contract.

Data Analysis and Interpretation of Fifty Respondents

The survey was conducted using a Google Form with responses from 50 participants.

- Among the respondents, 34 were male and 15 were female. The majority, 40 respondents, belonged to the age group of 18 to 30 years. Five respondents were aged between 30 and 40 years, three were under 18, one was between 40 and 50 years, and one respondent was above 50 years. Most of the respondents were students.
- Responses regarding the usage of online banking varied. A total of 44 respondents reported using online banking systems in their daily lives. Five respondents do not use online banking due to security concerns, while one respondent was unsure about using it.
- Out of 50 respondents, 47 had bank accounts.
- Regarding preferred modes of payment, 14 respondents still relied on cash for their transactions. Debit cards were used by 13 respondents, while only 2 used credit cards. Internet banking was used by 5 respondents, and mobile banking by 11 respondents. Cheques and e-wallets were used by 3 and 2 respondents respectively. The data indicates a growing trend in the use of mobile banking among Indian banking customers.
- Out of 50 respondents, 36 were aware of cybercrimes, while the remaining were either unaware or unsure.
- When asked about specific types of cybercrimes, 19 respondents had heard of hacking, making it the most commonly recognized cybercrime. Sixteen respondents were aware of banking or credit card-related cybercrimes, having learned about them through various sources.
- Regarding perceived reasons for bank account insecurity, 16 respondents identified cybersecurity issues as the primary cause. Eleven respondents cited fraud exposure in banks. Virus attacks and internet-related threats were equally noted by 10 respondents each. Additionally, 3 respondents attributed management-related threats as a cause.
- Nine respondents believed that the COVID-19 pandemic influenced their decision to start using online banking.
- In terms of trust, 35 respondents expressed faith in public sector banks, while 11 favored private sector banks.
- Twelve respondents admitted to having no awareness about cybersecurity issues, highlighting a gap in education and awareness.
- Concerning the most dangerous cyberattacks facing Indian banks, 16 respondents identified the theft of confidential data as the top threat. Data corruption was considered the second most dangerous by 12 respondents. Malware attacks and identity theft were each seen as critical threats by 5 respondents.
- When asked about the best security tools to protect online banking, 23 respondents favored biometric methods such as retinal scans, fingerprints, and voice recognition. Sixteen respondents believed passwords offer adequate protection. Seven respondents chose digital electronic signatures, and 4 respondents preferred digital electronic certificates as the best security tools.
- Twenty-three respondents were aware of the Cyber Security Protection Act.
- Thirty-five respondents reported never having experienced a cyber threat, while 9 respondents admitted to having experienced such threats. Six respondents preferred not to disclose their experiences.

Conclusion

Banks must prioritize addressing cybersecurity concerns within their online banking services, especially since many customers hold bank accounts but remain unaware of cybercrimes and the potential harm these attacks can cause. While most people recognize the importance of the Cyber Protection Act for Indian banks and are increasingly using online banking—contributing significantly to India's digitalization—there is still a sizable portion of the population that prefers cash payments and lacks awareness about digital security. The COVID-19 pandemic accelerated the adoption of digital payments, but with this shift, cyberattacks on banks surged by 238% between February and April 2020. In response, the Reserve Bank of India established the Reserve Bank Information Technology Private Limited (ReBIT) to manage IT and cybersecurity needs for Indian banks. It is crucial for banks to conduct comprehensive education and awareness programs to better inform customers about cybersecurity threats and preventive measures.

Furthermore, trust in public sector banks remains higher compared to private and foreign banks in India. To create a safer digital ecosystem, the central government must enhance cyber hygiene among all end-users, supported by coordinated efforts from the Centre Emergency Response Team (CERT-In). Banks themselves need to maintain rigorous cyber hygiene practices, including deploying effective anti-malware solutions to protect their systems. Another urgent area of focus is expanding insurance coverage for cyberattacks, as the rise in malware threats poses increasing operational and security risks. Ultimately, banks must actively educate their customers about cyber threats and the necessary precautions to safeguard sensitive data, ensuring a secure banking environment in an evolving digital landscape.

REFERENCES

1. Deborah Golden and Irfan Saif, ―The future of cyber survey 2019‖, Deloitte, 2019, https://www2.deloitte.com/us/en/pages/advis ory/articles/ future-of-cyber-survey.html
   https://www2.deloitte.com/content/ dam/Deloitte/covid19
2. https://www.rbi.org.in/Scripts/BS_PressRele aseDisplay.
3. http://www.compitjournal.org/paper/348/a-literature-review-on-cyber-securityin-indian- context
4. Simi. bajaj, 'cyber fraud: A digital crime, 'www.academia.edu/cyber_fraud_a_digital_ crime
5. www.researchgate.net
6. www.rebit.org.in
7. https://www.researchgate.net/publication
8. www.mananprakashan.com