International Journal of Research Publication and Reviews

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

Cyber Security Challenges in Indian Banks

Daksh Kumar

Galgotias University

Introduction

There is a big digital change happening in the Indian banking sector. The Unified Payments Interface (UPI), mobile banking apps, artificial intelligence (AI), and centralised core banking systems are just a few examples of how technology has changed the way people use and receive financial services. These improvements have made things better for customers and made operations run more smoothly. They have also made it much easier for cybercriminals to attack. Phishing, ransom ware, data breaches, and threats from inside the company are all becoming more common. This report looks at the range of cyber threats that Indian banks face, assesses how ready they are to deal with them, and suggests ways to make them more resilient to cyber-attacks.

Background and Rationale

More digital banking has made banks more open to new threats. Cybercriminals have started to target the financial services industry because it handles more than a billion UPI transactions every month and banks have established relationships with fintech ecosystems. The 2018 Cosmos Bank hack, which cost ₹94 crore because ATM servers were used in the attack, shows how vulnerable the sector is. CERT-In reported more than 13 lakh cyber incidents in 2022, many of which targeted banks. This shows how important it is to improve digital security systems. As cyber threats get more advanced, using technologies like AI and machine learning, banks need to strengthen their security measures in order to keep people's trust and keep the system stable.

Aims of the Research

- Evaluate the current state of cyber security infrastructure across Indian public and private sector banks
- Identify the most common and emerging cyber threats affecting the Indian banking ecosystem
- Assess the extent of compliance with RBI’s cyber security frameworks and guidelines
- Examine customer awareness regarding cyber risks and safety practices
- Recommend strategic, actionable solutions to improve institutional and customer cyber hygiene

Scope and Limitations

This study is mostly about Scheduled Commercial Banks (SCBs), with a focus on their branches in cities. It doesn't include Regional Rural Banks (RRBs) or cooperative banks, which may have their own weaknesses and lack of resources. Fifty people, including bank employees and customers, took part in the sample. Access to real-time incident data was limited because the subject was so sensitive. Also, because cyber threats change so quickly, research results need to be updated often.

Literature Review Highlights

- **CERT-In (2023):** A 47% surge in cyber incidents affecting the BFSI sector
- **RBI Cyber Security Framework (2016):** Mandated the creation of Board-approved security policies and operational SOCs
- **NCIIPC (2021):** Identified BFSI as part of critical national infrastructure
- **KPMG Cybercrime Survey (2021):** Insider threats cited as a top concern by 74% of bank respondents

- **IIM Ahmedabad Study (2020):** Advocated for integrating behavioural training in security frameworks
- **ISO/IEC 27001 & NIST:** Serve as international standards for security management best practices

Research Methodology

A mixed-method approach combining qualitative and quantitative techniques was adopted:

Primary Data Collection:

- **Structured Questionnaires:** Administered to 30 bank employees in IT, compliance, and operations
- **Interviews:** Conducted with 5 senior cyber security officers to capture organizational perspectives
- **Customer Surveys:** 20 banking customers across four metro cities assessed for awareness and experiences

Secondary Data Sources: RBI circulars, CERT-In reports, published case studies, and consulting firm whitepapers

Data Analysis Tools: Excel for tabulation and visualization, SPSS for statistical analysis, NVivo for thematic coding

Sampling: Stratified random sampling ensured representation from public and private banks, and various departments

Comparative Performance Analysis

Performance Metric	Public Sector Banks (PSBs)	Public Sector Banks (PSBs)
Threat Detection Speed	Moderate	Fast
Incident Response Plan	Semi-structured	Structured
Frequency of Security Audits	Annual	Quarterly
Employee Cyber Training	Annually	Quarterly
Customer Awareness Efforts	Low	Moderate to High

Comparative Regulation Compliance

Regulatory Area	PSBs Compliance	PVBs Compliance	Key Challenges
RBI Cyber Security Guidelines	65%	85%	Legacy systems, delayed implementation
Data Localization (2018)	Moderate	High	Cloud integration and migration issues
KYC/AML Procedures	High	High	Fraudulent/synthetic identities
IT Governance Frameworks	Low–Moderate	Moderate–High	Talent shortages, weak policy enforcement

Investment Trends Comparison

Area	PSBs (%)	PVBs (%)
Endpoint Protection	18	24
AI-Based Threat Detection	10	20
Employee Training	8	14
SOC/Incident Response	12	18
Customer Awareness Programs	5	10
Backup & Recovery Systems	10	12

Key Findings

1.Not enough customers know about it

A large number of banking customers, about 74%, don't know basic cyber hygiene rules like how to spot phishing emails, set strong passwords, avoid public Wi-Fi for financial transactions, and spot fake links or messages. This lack of knowledge makes cyber-attacks much more likely to work because customers are often the weakest link in the security chain. Customer carelessness can put even the most secure banking systems at risk if they don't get the right education or help.

2. Public sector banks (PSBs) have old infrastructure.

A lot of public sector banks still use old systems and IT infrastructure, which makes them more vulnerable to cyber threats. These systems don't always have the flexibility and scalability needed to deal with modern cyber-attacks, which makes threat detection, incident response, and patch management slower and less effective. As cybercriminals get better at using tools, these old systems become a big target.

3. Training that doesn't happen often enough or isn't good enough

Cyber security training for employees, especially in PSBs, is often not done on a regular basis, is not up to date, or is seen as a formality. This makes it hard for employees to stay up to date on the latest threats and protocols. Employees are more likely to fall for phishing scams or accidentally share sensitive information if they don't get regular training. This makes the bank's human-layer defences weaker.

4. Not following the rules set by the government

a lot of banks, especially those in the public sector, don't fully follow the rules set by the Reserve Bank of India (RBI). This is especially true when it comes to setting up a fully functional Security Operations Centre (SOC), doing audits on time, and putting in place strong cyber security frameworks. Not following the rules not only puts the bank at risk from outside threats, but it also hurts its reputation and costs it money in fines.

5. AI and automation are taking a long time to catch on

AI and machine learning can greatly improve threat detection, fraud prevention, and incident response, but PSBs are still slow to adopt them. This is mostly because of a lack of money, skilled workers, and the right technology. Because of this, these banks can't use real-time threat intelligence and predictive analysis to stop cyber threats before they happen.

Recommendations

1) Mandatory Cyber security Training Every Three Months Banks should require all employees to take cyber security training that is specific to their jobs every three months. These programs should have real-life simulations, phishing drills, and information on new threats and best practices. Regular, hands-on training helps create a workforce that is aware of security issues and lowers the risk of human error, which cybercriminals often take advantage of.

2) Monitoring Systems Powered by AI Banks need to spend money on advanced, AI-powered cyber security tools that can find anomalies in real time, analyse behaviour, and model threats before they happen. These systems can find strange patterns, mark activities that seem suspicious, and respond to threats faster than doing it by hand. Over time, adding AI can cut down on response times by a lot and stop big breaches from happening.

3) Platform for Sharing Threat Intelligence Led by RBI The Reserve Bank of India should set up a central platform for sharing threat intelligence that lets all banks—public, private, and cooperative—report and get information on the latest cyber threats, weaknesses, and ways to protect themselves. This kind of platform would encourage people to work together, help them understand what's going on, and support a unified, sector-wide approach to cyber defence.

4) Programs to raise customer awareness of cyber security Banks and other financial institutions should start big campaigns to raise awareness about cyber security among all types of customers. These programs need to be available in more than one language and use different types of media, like videos, info graphics, social media, email newsletters, and text messages. The goal is to teach customers about safe banking, new types of fraud, and how to avoid them.

5) Support for Public Sector Banks (PSBs) to modernise their IT Because PSBs don't have a lot of money, the government should set aside money to update their IT systems. This includes getting rid of old hardware and software, moving to cloud-based systems, and using cyber security tools that are both scalable and effective. Modern infrastructure not only makes things safer, but it also makes the quality of service better overall.

6) More strict oversight and enforcement of rules Regulators like the RBI should make sure that cyber security audits, frameworks, and incident response preparedness are more closely watched to make sure that they are being followed. Banks that put off implementing new rules or get bad audit results should have to pay fines and have their audit results made public. This will make them more accountable and speed up compliance.

7) Security audits by a third party that isn't connected to the company all banks should have to have certified outside cyber Security Company’s check their security every year. These audits should include thorough penetration testing, vulnerability assessments, and red teaming exercises. Independent evaluations help find blind spots and make sure that internal teams don't miss important weaknesses.

8) Multi-Factor Authentication (MFA) is required.

Multi-factor authentication should be required for both customers and employees to protect access to sensitive data and systems. This includes hardware tokens, biometrics, one-time passwords (OTPs), and authenticator apps. MFA makes it much less likely that someone will be able to get in without permission, even if their login information is stolen.

Summary

Cyber security has become a very important and growing issue in the Indian banking sector, especially for public sector banks (PSBs), which still have problems with old systems, limited technology, and not enough money. Because of these problems, PSBs find it hard to find, stop, and respond to advanced cyber threats. Private sector banks, on the other hand, have been more flexible and have invested in advanced cyber security tools, automation, cloud integration, and employee training programs ahead of time. Their way of doing things has usually made them better able to deal with cyber threats and respond to them faster.

The Reserve Bank of India (RBI) has put out a lot of good rules for managing cyber risks, like the Cyber Security Framework for Banks (2016). However, these rules are not always followed by all institutions. Many banks, especially those in the public sector, don't have the money or the will to fully follow these rules. This makes the sector as a whole less secure.

A full and coordinated plan is needed to deal with these growing threats in a way that works. This includes:

Updating technology, like getting rid of old infrastructure and using AI-based systems to find threats;

Programs that focus on people, like training employees regularly and making customers aware of their rights, can help reduce risks caused by human error.

And strict enforcement of rules, making sure that banks follow the rules by doing audits, punishing those who don't, and working together across the industry.

By following this three-pronged plan, Indian banks can greatly improve their cyber resilience, keep sensitive financial data safe, and keep the public's trust in the financial system, which is becoming more and more digital. It is not only necessary from a technical point of view, but also from a strategic point of view, for India's banking future to strengthen cyber security.