WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Cybersecurity Risk in Banking and Financial Services: An Analysis of Indian Financial Institutions

Kridip Das[1], Prof. Dr. Saumya Vatsyayan[2]

[1] MBA, Galgotias University
[2] Under the guidance of

ABSTRACT :

The rapid digitization of banking and financial services has significantly enhanced efficiency but also introduced complex cybersecurity risks. This study evaluates how Indian financial institutions manage these risks amidst increasing cyber threats. Through a hybrid research design involving literature review, industry case analysis, and conceptual survey data, we examine institutional preparedness, technological adoption, regulatory compliance, and human factors in cybersecurity. The findings suggest that while technical measures like multi-factor authentication (MFA) are widely adopted, gaps persist in employee training, incident response, and governance. This paper offers strategic recommendations for enhancing cybersecurity resilience in India's BFSI sector.

Keywords: Cybersecurity, Banking, Financial Services, Risk Management, India, BFSI, Phishing, Compliance, Incident Response, Training

1. Introduction

The Indian banking sector's digital transformation—driven by UPI, Aadhaar, and fintech integration—has increased vulnerability to cyber threats. High-profile attacks and phishing incidents underscore the need for robust cybersecurity frameworks. Despite regulatory initiatives, the gap between compliance and effective cyber risk mitigation remains significant.

2. Research Objectives and Questions

Objectives:
- Identify major cyber threats to BFSI institutions
- Assess impact of training and compliance on breach rates
- Evaluate AI and automation tools in breach detection
- Recommend actionable strategies for cyber resilience

Research Questions:
- What are the most common cyber threats in Indian banking?
- Does employee training correlate with fewer phishing breaches?
- How effective are current compliance frameworks (RBI, NIST, ISO)?
- Are Indian banks prepared to detect and recover from attacks?

3. Methodology

A mixed-method approach was adopted:
- Exploratory research: Literature reviews, RBI/CERT-In reports, case studies (e.g., Cosmos Bank)
- Descriptive design: A conceptual survey (n=200) of IT/security professionals across public, private, and cooperative banks
- Data Analysis: Frequency distributions, cross-tabulations, and visualization

4. Key Findings

Cybersecurity Practice	Adoption Rate
Multi-Factor Authentication (MFA)	88%

Regular Training | 65%
Incident Response Plan | 60%
Compliance with Frameworks | 78%
Cyber Incidents Reported | 42%

- Training Effectiveness: Institutions with quarterly training reported fewer phishing cases.
- Compliance Impact: Compliance with RBI/ISO frameworks correlated with higher preparedness scores.
- AI Adoption: Limited use of AI tools hinders real-time threat detection.

5. Discussion

Technical tools alone are insufficient; human factors and governance matter. Employee awareness remains low, particularly in rural branches. Smaller banks lag behind in adopting best practices due to budget and talent constraints. Leadership involvement and cross-functional planning improve breach response.

6. Limitations

Simulated survey data; no access to live bank data. Non-random sampling. Results are indicative, not definitive.

7. Recommendations

1. Board-Level Cyber Governance
2. Quarterly Awareness Campaigns and Simulations
3. Upgrade Legacy Infrastructure with AI-Powered Security Tools
4. Vendor Risk Audits and Cybersecurity Clauses
5. Customer Education Programs in Local Languages

8. Conclusion

Cybersecurity in BFSI must evolve from a compliance task to a strategic function. While Indian banks are making progress, a layered, resilience-driven approach is essential. Institutions must invest in technology, people, and policies simultaneously to withstand the rising tide of cyber threats.

REFERENCES

- Accenture (2023). Cybersecurity in Banking
- Von Solms & Van Niekerk (2013). Computers & Security
- RBI (2016). Cyber Security Framework in Banks
- CERT-In (2022). Annual Report
- NIST (2022). Cybersecurity Framework
- IBM X-Force (2023), KPMG India (2022), Deloitte (2022)