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

Golu Kumar

MBA Student School of Business Galgotias University, Greater Noida

ABSTRACT :

Cybersecurity is a critical issue in the banking and financial services sector, driven by rapid digital transformation and increasing cyber threats. This paper explores the types of cyber risks banks face, including phishing, ransomware, insider threats, and third-party vulnerabilities. It also examines the effectiveness of current defense mechanisms, such as encryption, multi-factor authentication, and regulatory compliance frameworks like RBI guidelines and GDPR. Using a mixed-method approach that includes surveys and expert interviews, the study highlights major gaps in employee awareness and third-party risk management. It concludes with strategic recommendations for improving cyber resilience.

KEY WORDS: Cybersecurity, Banking, Financial Services, Risk Management, Data Breach, Compliance

INTRODUCTION

The rise of digital banking has introduced both convenience and cybersecurity challenges for financial institutions. With increasing cyber threats targeting sensitive data, the banking sector is under constant pressure to adopt robust security practices. This section introduces the importance of cybersecurity, the growing threat landscape, and the need for proactive risk management in banking.

LITERATURE REVIEW

The literature highlights common threats such as phishing, malware, and insider breaches, and emphasizes the importance of regulatory frameworks (RBI, PCI-DSS, GDPR). Researchers note the adoption of tools like multi-factor authentication, AI-based threat detection, and the role of human behavior in cybersecurity effectiveness. Despite advances, gaps remain in training, third-party security, and real-time response.

METHODOLOGY

This study uses a mixed-method approach, combining surveys and interviews with secondary data analysis. Quantitative data was collected via structured questionnaires sent to banking professionals, while qualitative insights were obtained through semi-structured interviews. The factor rating method was used to evaluate and prioritize cybersecurity measures.

DATA COLLECTION

Primary data was gathered from 40 banking professionals and 6 cybersecurity experts. Secondary data included journal articles, regulatory publications, and industry reports. The survey focused on identifying key threats, preparedness levels, and security tools in use, while interviews explored deeper insights into strategy, challenges, and future planning.

ANALYSIS AND RESULT

Survey analysis showed phishing and ransomware as the most frequent threats. Multi-factor authentication and data encryption were the most widely used countermeasures. Employee training and third-party risk were ranked low. Interviews confirmed that most banks take a reactive rather than proactive security stance and struggle with vendor compliance and resource allocation.

DISCUSSION

While banks have implemented strong technical defenses, non-technical vulnerabilities persist. Human error, lack of training, and vendor risks were found to be major weak spots. Compliance is improving, but often lacks strategic integration. Recommendations include adopting a layered security approach, enhancing training, using AI tools, and involving top management in cyber governance.

CONCLUSION

Cybersecurity in banking is a multifaceted challenge requiring both technological and human-centered solutions. This research shows that while progress has been made, significant work remains in employee awareness, vendor management, and real-time threat detection. Institutions must prioritize cybersecurity as a strategic goal, not just an IT issue, to safeguard trust and financial integrity in the digital age.

REFERENCE

1. IBM Security (2022). Cost of a Data Breach Report.
2. Deloitte (2022). The Future of Cybersecurity in Financial Services.
3. PwC (2023). Global Digital Trust Insights.
4. Reserve Bank of India (2016). Cybersecurity Framework in Banks.
5. Verizon (2023). Data Breach Investigations Report.
6. GDPR (2018). Regulation (EU) 2016/679.