International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Cybersecurity Risk in Banking and Financial Services

ANKIT OJHA[*1], DR. SITANSU PANDA [*2]

[1]Researcher, Department of Management, School of Business, Galgotias University [*2]

Guide, Department of Management, School of Business, Galgotias University

1. Overview

Unprecedented convenience and efficiency have been brought about by the banking and financial services sector's fast digital transformation, but there is also a greater risk of cyberattacks. Banks now face increased risks including ransomware, phishing attacks, data breaches, and insider threats as a result of the integration of technology like cloud services, fintech platforms, and mobile banking.

In India, cybersecurity issues still exist because of antiquated IT systems, inadequate training, and sluggish incident response, even with legal frameworks like the RBI's Cyber Security Framework (2016). This vulnerability was exacerbated by the COVID-19 pandemic, which is why a comprehensive and strategic cybersecurity approach is more important than ever.

2. Review of Literature

Sources from academia and business emphasize how serious cyber threats are. IBM (2023) estimates the average cost of a data breach in financial services at $5.9 million. While Böhme and Moore (2012) emphasize the importance of risk-based investments, scholars such as Dhillon and Backhouse (2001) support cybersecurity governance at the board level.

Significant events, such as the Capital One data leak in 2019 and the Bangladesh Bank SWIFT breach in 2016, show how little technical errors may have a big impact. These incidents demonstrate that without operational preparedness, employee awareness, and real-time monitoring, regulatory compliance is insufficient on its own.

3. Research Goals and Theories

Goals

Determine the main cyberthreats that banks face.

Examine the connections between investing in cybersecurity and preventing breaches.

• Assess how employee training affects cyber incidents.

Evaluate how well incident response plans are working.

• Recognize how cybersecurity maturity is impacted by regulatory compliance.

Theories

• H1: Less cyberattacks result from increased cybersecurity investment.

• H2: Fewer phishing attempts result from increased employee training.

• H3: Plans for incident reaction → Quicker recuperation.

• H4: Stricter cybersecurity procedures resulting from regulatory compliance.

4. Methods of Research

Both descriptive and exploratory designs were employed in the study:

• Examined case studies, industry white papers, and RBI recommendations during the exploratory phase.

• Descriptive Phase: 200 simulated replies were examined to identify patterns and connections in cybersecurity procedures.

Banking professionals were fictitiously given a survey in the form of a questionnaire. Nominal, ordinal, and frequency scales were used to measure the responses.

Simulated Results:

• There were fewer breaches at banks that made greater investments in cybersecurity.

Why Organizations that regularly trained their staff experienced fewer phishing attacks.

Increased cybersecurity maturity was associated with higher regulatory compliance, and formalized incident response procedures sped up post-breach recovery.

5. Important Cyberthreats Recognized

Phishing is the practice of deceiving users through fraudulent emails or communications.

Programs created to steal or lock data are known as malware or ransomware.

• DDoS Attacks: When systems are overloaded, services are interrupted.

• Insider Threats: Workers abusing their position.

• Advanced Persistent Threats: Long-term, covert assaults.

6. Suggestions

1. Invest Strategically: Consider spending on cybersecurity as a strategic imperative rather than a burdensome regulatory requirement.

2. Employee Education: Provide continuous, engaging instruction on response procedures, phishing simulation, and cyber hygiene.

3. Tested Incident Response Plans: Create and practice recovery procedures to reduce data loss and downtime.

4. Compliance as Culture: Include regulatory standards such as ISO and RBI's Framework in corporate procedures.

5. Customer Awareness: Start initiatives to inform consumers about safe banking practices and cyber crimes.

6. Threat Intelligence Sharing: Work together with colleagues in the industry to exchange threat intelligence and improve collective defense.

7. Restrictions

• Because of practical limitations, simulated data was utilized.

• Since the results are conceptual, they shouldn't be extrapolated without first-hand data verification.

• Organizational culture, employee conduct, and real-time situations can all differ.

8. In conclusion

In the banking industry, cybersecurity is not only a technological issue but also a strategic necessity. A multifaceted strategy including technological defenses, employee training, regulatory alignment, real-time monitoring, and robust governance is needed to safeguard financial assets and customer trust.

The essential roles that investment, awareness, readiness, and compliance play in lowering cyber risk in financial services are highlighted by the conceptual support for the research's hypotheses.