iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79493

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Cyber Security Management in Financial Organizations of Bangladesh: Challenges, Strategies, and Future Directions

Md. Abu Nahee Ibna Zahid[1], Halima Akter Beli[2]
[1]*IT Professional, Private Commercial Bank, Bangladesh*
[2]*ICT Tutor, Private College, Bangladesh*

Abstract: ***The rapid digital transformation of financial institutions has significantly improved banking efficiency and accessibility in Bangladesh. However, this transformation has also increased exposure to cyber threats targeting sensitive financial information and digital banking infrastructures. The financial sector in Bangladesh has experienced several high-profile cyber incidents, highlighting the urgent need for effective cybersecurity management frameworks. This research paper examines the current cybersecurity landscape in financial organizations of Bangladesh, identifies major cyber threats and vulnerabilities, evaluates existing cybersecurity policies, and proposes strategic improvements for strengthening cybersecurity governance. Using secondary data sources, reports from regulatory authorities, and global cybersecurity frameworks, the study explores the institutional readiness of financial organizations to mitigate cyber risks.***

The findings indicate that although Bangladesh Bank and financial institutions have introduced cybersecurity guidelines and technological safeguards, significant gaps remain in infrastructure, human resource expertise, and threat monitoring capabilities. The study concludes with policy recommendations including stronger regulatory enforcement, investment in cybersecurity infrastructure, workforce development, and adoption of international cybersecurity standards to ensure a resilient financial ecosystem.

Keywords: Cybersecurity, Financial Institutions, Bangladesh Banking Sector, Cyber Risk Management, Digital Banking, Information Security.

I. INTRODUCTION

The financial sector is one of the most critical components of any modern economy. In Bangladesh, financial institutions—including commercial banks, non-bank financial institutions (NBFIs), and mobile financial service providers—have undergone significant digital transformation during the last decade. The rapid adoption of digital banking, online payment systems, and mobile financial services has enhanced financial inclusion and operational efficiency. However, these technological advancements have also increased exposure to cyber threats and digital fraud.

Cybersecurity has therefore become a critical priority for financial organizations worldwide. Financial institutions store and process sensitive customer data, making them prime targets for cybercriminals. According to global cybersecurity reports, financial institutions experience some of the highest levels of cyberattacks compared to other sectors [1].

In Bangladesh, the importance of cybersecurity became particularly evident after the Bangladesh Bank heist of 2016, where hackers attempted to steal nearly $1 billion through the SWIFT network and successfully transferred $81 million from the central bank's account at the Federal Reserve Bank of New York [2]. This incident exposed serious weaknesses in cybersecurity management within the country's financial sector and triggered a nationwide policy response to strengthen digital security.

Since then, Bangladesh Bank has issued several cybersecurity guidelines. As per the Information and Communication Technology (ICT) Security Guidelines for Banks and Non-Bank Financial Institutions, require financial institutions to adopt risk management frameworks, cybersecurity monitoring mechanisms, and data protection strategies [3].

Despite these efforts, cyber threats continue to evolve rapidly. Financial organizations face multiple challenges such as phishing attacks, malware infections, insider threats, ransomware attacks, and distributed denial-of-service (DDoS) attacks. In addition, the increasing popularity of mobile financial services such as bKash, Nagad, and Rocket has expanded the attack surface for cybercriminals.

This research paper investigates cybersecurity management practices in financial organizations in Bangladesh, focusing on:

1) The current cybersecurity landscape.
2) Major cyber threats affecting financial institutions.
3) Existing cybersecurity policies and regulatory frameworks.
4) Key challenges faced by financial organizations.
5) Strategic recommendations for strengthening cybersecurity resilience.

II. LITERATURE REVIEW

Cybersecurity has become a critical issue for financial institutions due to the increasing sophistication of cyber threats and the expanding digital ecosystem of financial services. According to Von Solms and Van Niekerk, cybersecurity management involves not only technological solutions but also organizational policies, risk management frameworks, and human awareness programs [4].

The financial sector is particularly vulnerable to cyberattacks because of the high monetary value associated with financial transactions. Studies show that cybercriminals frequently target banks and financial institutions through malware, phishing campaigns, and ransomware attacks [5].

Developing countries face greater cybersecurity challenges due to limited technological infrastructure, shortage of cybersecurity professionals, and insufficient regulatory enforcement. In the context of Bangladesh, many banks have lack comprehensive cybersecurity governance frameworks and rely heavily on reactive security measures rather than proactive risk management strategies.

The Bangladesh Bank cyber heist has been widely analysed in cybersecurity literature. According to reports from international cybersecurity firms, the attack exploited vulnerabilities in the bank's network security, outdated hardware, and lack of proper firewall protection.

Another important issue highlighted in the literature is the growing risk associated with mobile financial services. With millions of users relying on mobile payment systems, cybersecurity threats targeting mobile platforms have increased significantly.

Global cybersecurity frameworks such as ISO 27001, NIST Cybersecurity Framework, and COBIT provide comprehensive guidelines for managing information security risks in financial organizations [6].

However, many financial institutions in developing countries have not fully implemented these frameworks due to cost constraints, lack of expertise, and insufficient regulatory pressure.

III. CYBERSECURITY LANDSCAPE IN BANGLADESH'S FINANCIAL SECTOR

A. *Digital Transformation in Banking*

Bangladesh has experienced rapid growth in digital financial services over the past decade. According to Bangladesh Bank statistics, the number of internet banking users and mobile financial service transactions has increased significantly.

Mobile financial services have particularly transformed the financial landscape by enabling millions of people to access financial services through smartphones and feature phones.

B. *Cyber Threat Statistics*

The cybersecurity threat landscape in Bangladesh has intensified in recent years. Reports indicate that financial institutions face hundreds of cyber intrusion attempts every day.

Cybersecurity monitoring systems have identified several sources of cyberattacks targeting Bangladesh's financial institutions. Many attacks originate from foreign locations, including East Asia and Eastern Europe.

C. *Common Cyber Threats*

Financial institutions in Bangladesh face multiple types of cyber threats, including:

1) Phishing Attacks: Phishing attacks involve fraudulent emails or messages designed to trick users into revealing sensitive information such as passwords and banking credentials.
2) Malware Attacks: Malware can infiltrate financial systems and allow attackers to gain unauthorized access to confidential data.
3) Ransomware: Ransomware attacks encrypt organizational data and demand payment for decryption.
4) Distributed Denial-of-Service (DDoS): DDoS attacks overwhelm servers with excessive traffic, disrupting online banking services.
5) Insider Threats: Employees with authorized access to systems may intentionally or unintentionally cause security breaches.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

IV. CYBERSECURITY MANAGEMENT FRAMEWORKS

Effective cybersecurity management requires a structured framework integrating technology, governance, and human factors.

1) *Risk Management:* Financial institutions must identify potential cyber risks and implement risk mitigation strategies.
2) *Security Policies:* Organizations should develop clear cybersecurity policies covering data protection, network security, and access control.
3) *Security Awareness Training:* Employee awareness is critical for preventing cyber incidents.
4) *Incident Response Planning:* Organizations must establish incident response teams capable of detecting and responding to cyber incidents quickly.

V. REGULATORY FRAMEWORK IN BANGLADESH

The Government of Bangladesh has introduced several regulations to strengthen cybersecurity in the financial sector.

A. Bangladesh Bank ICT Security Guidelines

These guidelines require banks to implement strong authentication mechanisms, encryption systems, and cybersecurity monitoring tools.

B. Digital Security Act

The Digital Security Act provides legal mechanisms for combating cybercrime and protecting digital infrastructure.

C. National Cybersecurity Strategy

The government has developed a national strategy aimed at improving cybersecurity awareness, infrastructure, and institutional coordination.

VI. CHALLENGES IN CYBERSECURITY MANAGEMENT

Despite regulatory efforts, financial organizations face several challenges:

1) Shortage of cybersecurity professionals
2) Limited cybersecurity budgets
3) Outdated IT infrastructure
4) Insufficient threat intelligence sharing
5) Lack of employee cybersecurity awareness

VII. RECOMMENDATIONS

To strengthen cybersecurity management, financial institutions in Bangladesh should adopt the following strategies:

1) *Adoption of International Standards:* Banks should implement international standards such as ISO 27001.
2) *Cybersecurity Investment:* Financial institutions must allocate greater budgets to cybersecurity technologies.
3) *Workforce Development:* Training programs should be developed to produce skilled cybersecurity professionals.
4) *Cyber Threat Intelligence Sharing:* Banks should collaborate with regulators and cybersecurity agencies to share threat intelligence.
5) *Continuous Monitoring:* Advanced threat detection systems should be implemented to monitor cyber threats in real time.

VIII. CONCLUSION

Cybersecurity has become a critical component of financial stability in Bangladesh. The increasing adoption of digital banking services has expanded the cyber threat landscape, making financial institutions more vulnerable to cyberattacks.

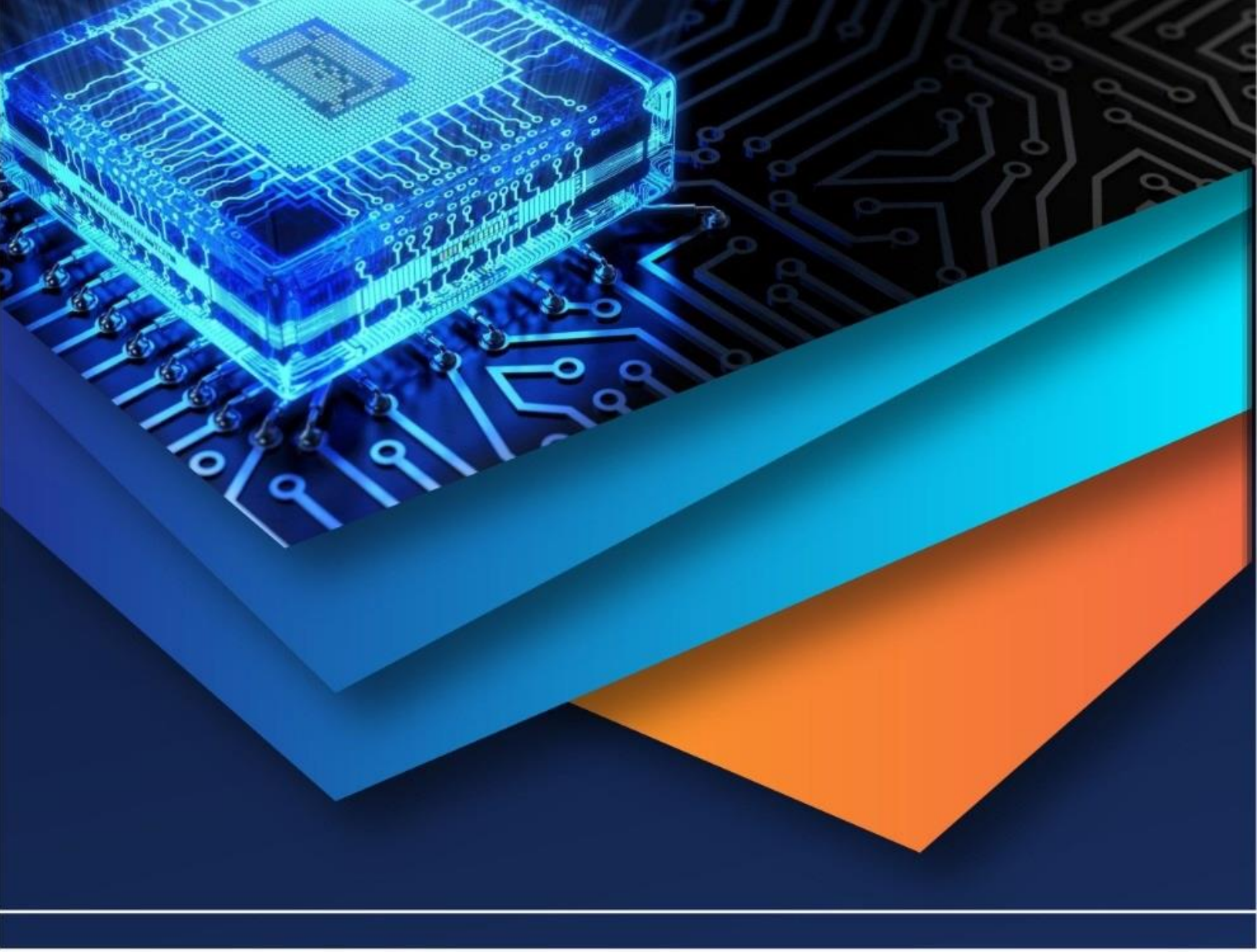
Although Bangladesh has taken important steps to strengthen cybersecurity governance, several challenges remain in terms of technological capability, human resources, and institutional coordination.

A comprehensive cybersecurity management strategy integrating technological safeguards, regulatory enforcement, and workforce development is essential for ensuring the resilience of Bangladesh's financial sector.

Future research should explore empirical analysis of cybersecurity preparedness across different financial institutions and evaluate the effectiveness of cybersecurity policies in preventing cyber incidents.

REFERENCES

[1] International Telecommunication Union (ITU). Global Cybersecurity Index 2020.
[2] M. Rahman, “A Forensic View of Bangladesh Bank Reserve Heist,” Sep. 2016.
[3] Bangladesh Bank. ICT Security Guidelines for Banks and Non-Bank Financial Institutions, 2023.
[4] R. V. Solms and J. V. Niekerk, “From Information Security to Cyber Security,” Computers & Security, vol. 38, pp. 97–102, 2013.
[5] Verizon. Data Breach Investigations Report, 2023.
[6] National Institute of Standards and Technology (NIST). Cybersecurity Framework, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY