Electronic Fraud (Cyber Fraud) Risk in the Banking Industry of Nepal

Sushil Mahato, Rakesh Kumar Nayak, Aryan Dipak Raut, Jyoti Yadav

Sambhram Institute of Technology, Bangalore, India'
Sambhram Institute of Technology, Bangalore, India'
National Academy(campus)

---***---

Abstract - The rapid adaptability of digital banking technologies in Nepal has exposed banks to increasingly rising risks of electronic fraud and cyber threats. In this paper, the authors investigate common types of cyber fraud faced, assess their impact on the banking sector, and propose a framework on how to mitigate these risks using global cybersecurity standards like the NIST framework. This research is therefore informed by data collected through surveys with banking professionals and secondary analysis of already existing incidents in Nepal. It highlights the vulnerabilities and suggests some robust strategies to protect Nepalese banks from cyber fraud.

Key Words: Cybersecurity in banking, digital banking threats, phishing attacks, AI-driven fraud detection, regulatory frameworks.

1.INTRODUCTION

The banking industry in Nepal plays a major role for economic stability and financial development. However, these changes are introducing a number of significant risks, especially in the sphere of cyber fraud. In particular, recent years have shown an appreciable rise in incidents of cyber frauds across the globe, and they really create problems for customers' confidence and operational efficiency. With resources constrained, limited technological advancements, and an ever-evolving threat landscape, these risks in Nepal are manifolds. All these vulnerabilities call for a proactive approach in safeguarding Nepalese banks' digital infrastructure. This research deals with the prevalent types of cyber fraud impacting Nepal's banking sector, assesses existing mitigation strategies, and presents the implementation of globally recognized frameworks to reduce these risks.

2. LITERATURE REVIEW

Electronic fraud encompasses phishing, malware attack, insider threats, and social engineering attacks. It is reported that Nepalese banks use very outdated systems with minimal protection layers. Researchers have identified the effectiveness of the NIST cybersecurity framework in improving risk mitigation globally. This research takes up such findings and applies them to the Nepalese context, addressing some of the identified vulnerabilities, including low cybersecurity awareness and poor regulatory compliance.

3. METHODOLOGY

The research design for this study adopts the mixed-method approach that blends both qualitative and quantitative data to offer an encompassing presentation of the risks associated with cyber fraud within the banking industry in Nepal.

3.A Primary Data Collection:

Surveys: To collect the required information, IT professionals, cybersecurity analysts, and employees working in Nepal's banking sector are administered questionnaires. It has a sample size of 100 respondents to take into consideration diversity regarding viewpoints across different levels of responsibility.

Objective: These surveys are designed to capture firsthand insights into the types of cyber fraud encountered, the effectiveness of current mitigation strategies, and the challenges faced in implementing cybersecurity measures.

3.B Secondary Data Collection

Reports and Studies: The data is sourced from official publications like Nepal Rastra Bank's annual reports and research studies focusing on the banking sector's cybersecurity.

International Case Studies: Compare with global practices to put into perspective and benchmark improvements in Nepal's cybersecurity infrastructure.

3.C Analysis Tools

SPSS, or Statistical Package for the Social Sciences, serves to analyze quantitative data from the surveys. It covers correlations, trends, and statistical relationships between variables such as the frequency of cyber fraud incidents and the effectiveness of mitigation strategies.

Benefits: SPSS will allow for strong interpretation of the data collected, hence bringing out patterns that inform recommendations.

3.D Framework Used

The NIST Cybersecurity Framework provides the basis for this analysis and recommendation of cybersecurity controls. NIST presents a well-organized process through five core functions: Identify, Protect, Detect, Respond, and Recover.

Application: The framework has been adapted to the Nepalese Banking context, especially on the enhancement of security protocols, risk assessment, and incident response mechanisms to suit local needs.

4. RESULTS

4.A Types of Cyber Fraud in Nepalese Banks

Based on the research findings, the most prevalent types of cyber fraud impacting Nepalese banks are:

Phishing 34% of incidents involved phishing, a cyber fraud method wherein attackers impersonate legitimate entities to deceive people into divulging sensitive information like passwords or account details. This is generally carried out through email and fake websites, targeting bank customers and employees alike.

Malware-based Fraud 26%

Malware attacks consist of the exploitation of malicious software with the intent of compromising a system, stealing data, or disrupting operations. Most times, these take place because a system is using an out-of-date system or has accessed malware-laden attachments through some phishing email.

Social Engineering: 20%

Social engineering fraud relies on tricking people into divulging confidential information and thereby evading technical security. Hackers use psychological manipulative tactics to mislead employees or customers, appearing as trusted authorities.

Insider Threats: 10%

Insider threats involve employees or contractors misusing internal system access for malicious uses. These cases are less frequent, but their influence on economic losses and damage to reputation is really huge.

4.B Key Vulnerabilities Identified

The research highlighted critical vulnerabilities in the Nepalese banking sector that exacerbate the risk of cyber fraud:

Lack of Multi-Factor Authentication (MFA):

Many banks are still dependent on single-factor authentication, which generally means password-based and prone to breach. Without MFA in place, attackers will find it much easier to reach into the system unauthorized. Poor.

Employee Training:

Employees are usually not well trained in identifying and reducing cyber threats, including phishing and social engineering attacks. This is a huge knowledge gap that increases the chances of human error causing cyber fraud.

Outdated Software Systems:

Several banks use old systems that are unable to cope with modern cybersecurity threats. Not being regularly updated, they remain vulnerable to attackers.

4.C Impact on Banking Operations

The consequences of cyber fraud are far-reaching, affecting both financial stability and consumer confidence:

Financial Losses:

In fact, Nepalese banks reportedly suffer a collective financial loss of around NPR 50 million annually due to cyber fraud. This estimate includes direct losses from fraudulent transactions and indirect costs, such as incident response and system recovery.

Decline in Consumer Trust:

A survey conducted in this regard has shown that 60% of customers feel insecure in using online banking services due to perceived risks in cybersecurity. This distrust may hamper the adoption of digital banking and reduce customer retention.

5. DISCUSSION

5.A Challenges

Nepal's banking sector faces significant challenges in combating cyber fraud, stemming primarily from limited resources, a shortage of skilled personnel, and inadequate government support:

Limited Resources: Most banks operate on a very low budget, which restricts them from investing in advanced cybersecurity technologies. Small and medium-sized banks have greater vulnerabilities because of not having a large enough budget for system upgrades or hiring cybersecurity specialists.

The Banking Sector Lacks Skilled Employees Who Can Develop and Implement Sophisticated Defense Mechanisms. This is usually very threatening because it often causes delay reactions towards emerging vulnerabilities.

Insufficient Support from the Government: Much as the regulatory framework in Nepal is still underdeveloped, so are enforcement mechanisms. A general absence of comprehensive national policies in computer security has left banks with no clear guidelines on the necessity for robust security measures.

5.B Opportunities

Despite these challenges, several opportunities exist for Nepalese banks to strengthen their cybersecurity posture:

Investment in Cybersecurity Tools: Advancing technology has brought new solutions to banks, including AI-powered fraud detection mechanisms and blockchain for added security in transactions.

Training Programs: Regular training for employees and IT staff can raise awareness of the threats and prepare them for the fight against cybercrime. The same or similar cybersecurity literacy programs can also be offered to customers to minimize risks related to phishing and social engineering attacks.

Adoption of Global Standards: The adoption of internationally recognized frameworks, such as the NIST Cybersecurity Framework, helps banks institute an organized way of approaching risk management and incident response.

5.C Comparison with Global Practices

A comparative analysis reveals that adopting global cybersecurity frameworks, such as the NIST Cybersecurity Framework, has proven effective in other countries:

Success of the USA: Most of the financial institutions in the United States have already started implementing the NIST framework, which has a straightforward structure based on five core functions: Identify, Protect, Detect, Respond, and Recover. This has greatly reduced the number of vulnerabilities and managed incident response mechanisms both in large and small organizations.

Relevance to Nepal: Even though the scale of operations is different, Nepalese banks can adopt the NIST framework according to their need, focusing on cost-effective measures and prioritizing critical risks. Such a tailored implementation could give solutions to challenges like scarce resources while aligning the organization with global best practices.

6. RECOMMENDATIONS

Policy Enhancements

To strengthen cybersecurity in Nepal’s banking sector, policy measures should be prioritized:

Compulsory Compliance on Cybersecurity: Regulators, such as Nepal Rastra Bank, must put in place strict guidelines on cybersecurity for all banks and financial institutions. For this, compliance should be compulsive to ensure at least a minimum level of security.

Regular Audits and Risk Assessments: Banks have to perform periodic audits and assessments of cyber risks to identify weak points and verify that the safety measures are at par with changing threats.

Technological Upgrades

Leveraging advanced technologies can significantly enhance a bank’s ability to detect and mitigate cyber threats:

AI-powered fraud detection systems can monitor massive transactional data to identify suspicious trends in real time and can help banks to prevent fraud beforehand.

Cloud-based Security Solutions: Migrating to secure cloud environments, scalability, and data protection will provide a robust system of defense against cyber threats with reduced dependence on obsolete in-house systems.

Employee Training

Human error is often the weakest link in cybersecurity. Regular training can equip employees with the knowledge to recognize and respond to threats effectively:

Workshops on Cyber Threats: Banks should organize periodic training sessions and workshops to educate employees about common cyber risks such as phishing, malware, and social engineering.

Simulated Exercises: Mock scenarios can help employees practice their response to cyber incidents, building their confidence and readiness.

Customer Awareness

Empowering customers to take precautions is crucial in minimizing cyber fraud risks:

Phishing Awareness Campaigns: Banks should undertake focused campaigns to educate their customers about phishing methods and how to check the authenticity of messages.

Safe Online Banking Practices: Clear advice on the safe handling of passwords, avoidance of public Wi-Fi for transaction processing, and the recognition of fraud sites will decrease customer vulnerability.

7. CONCLUSION

The Nepalese banking industry is facing an upward trend in cyber fraud risks that may cause instability in the sector. This research highlights the need for a full adoption of a cybersecurity framework. Global practices, such as the NIST framework, together with local adaptations, can bring about considerable reductions in vulnerabilities. This requires collaboration among banks, regulators, and customers to establish a secure banking environment.

8. REFERENCES

1. Maharjan, R., & Chatterjee, J. (2019). Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. *LBEF Research Journal of Science, Technology, and Management*.
2. Nepal Rastra Bank (2023). *Annual Financial Stability Report*.
3. National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity.
4. Rainer, R. K., et al. (2020). *Introduction to Information Systems*. McGraw-Hill Education.