CYBERSECURITY RISKS IN DIGITAL BANKING OPERATIONS IN VIETNAM: CURRENT SITUATION AND SOLUTIONS

Do Thi Thu Ha* - Nguyen Thanh Tung*

Abstract: ***In the era of Industry 4.0, cyberspace offers limitless potential for global integration and socio-economic development. However, cybersecurity risks have become a primary concern for internet users, particularly in the financial and banking sectors. As banks undergo digital transformation toward a fully digital banking model in the future, the application of digital technology brings numerous opportunities but also significantly increases the risk of cybercrime attacks. Therefore, effectively managing cybersecurity risks in digital banking operations in Vietnam has become an urgent matter. This paper provides a comprehensive overview of cybersecurity risks and their impacts on digital banking activities in Vietnam. It also clarifies the challenges in managing such risks and proposes several groups of solutions based on three main pillars: Processes, Technology, and People, along with compliance solutions related to cybersecurity risk prevention principles.***

• Keywords: *cybersecurity risks, cybercrime, digital banking.*

Date of receipt: 29th Aug., 2025
Date of delivery revision: 15th Sep., 2025
Date of receipt revision: 28th Oct, 2025
Date of approval: 21th Nov., 2025
DOI: https://doi.org/10.71374/jfar.v25.i6.05

1. Introduction

In recent years, cybercrime has escalated both in scale and sophistication. Reports from the FBI and international cybersecurity organizations show that cyberattacks surged sharply during and after the COVID-19 pandemic, with several types of attacks increasing by more than 300% and causing substantial economic losses globally. Cybersecurity Ventures estimates that global damages reached USD 6 trillion in 2021 and may rise to USD 10.5 trillion by 2025 levels comparable to the world's third-largest economy.

Within this landscape, the financial-banking sector remains one of the most attractive targets, as nearly 70% of financial institutions worldwide have experienced cyberattacks. IBM's 2023 Cost of Data Breach Report also ranks banking among the sectors with the highest loss magnitude, reflecting the industry's heavy reliance on digital platforms and continuous exposure to sophisticated threats.

Vietnam faces similar pressures. Although the number of recorded attacks fluctuates, the country consistently ranks among the most targeted in Southeast Asia. Data from the Ministry of Information and Communications show that over 95% of reported online fraud cases in the first half of 2023 were related to banking and finance. The National Cybersecurity Monitoring Center also detected thousands of attacks on information systems, many involving impersonation of banks or the creation of fraudulent websites.

As banks accelerate digital transformation to enhance operational efficiency and customer experience, their exposure to cyber risks deepens. Threats range from data breaches and unauthorized access to scams directly targeting customers through social engineering or falsified online interfaces.

Against this backdrop, this paper examines cybersecurity risks and their implications for digital banking operations in Vietnam. It identifies key shortcomings in current risk-management practices and proposes a set of solutions grounded in three core pillars processes, technology, and people together with recommendations to strengthen governance and compliance in line with cybersecurity risk-prevention principles.

2. Cybersecurity risks and digital banking activities

2.1. Cybersecurity risks

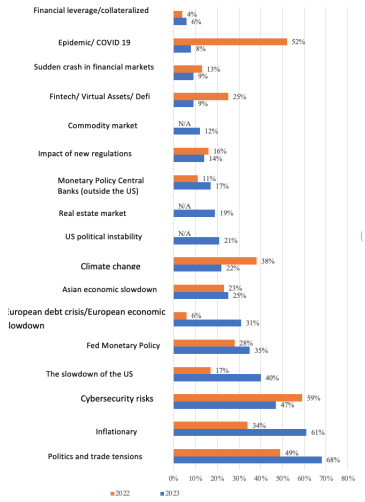
Cybersecurity risks, or cyber risks, refer to threats arising from the operation of information technology (IT) that negatively affect the confidentiality, availability, or integrity of an organization's technology or information systems (Cebula & Young, 2010). In simpler terms, cybersecurity risks are the potential for loss or damage resulting from breaches or attacks on an organization's IT systems, leading to technical infrastructure damage or misuse of digital technologies (Moyo, 2022).

In recent years, cybersecurity risks have garnered increasing attention from organizations worldwide. According to a 2023 survey by DTCC, cybersecurity

* *Banking Academy*

risk ranks among the top concerns threatening global financial system stability second only to political risks and trade tensions, and inflation risks (Figure 1).

Figure 1. Systemic risks affecting global financial system stability



Source: DTCC Survey (2023)

(*Note: Percentage indicates respondents who identified each factor as one of the top 5 systemic risks affecting financial system stability globally*)

2.2. Cybersecurity risks in the financial and banking sector

Due to the nature of the industry, where operations rely heavily on IT infrastructure, the financial and banking sector is one of the most attractive targets for cybercriminals. The number of malware attacks targeting banks and financial institutions surpasses all other industries, and attack methods are becoming increasingly sophisticated (Darem et al., 2023). Examples of major cyberattacks on banks and financial systems include (Aldasoro et al., 2021; Bouveret, 2018; Rojas Rincón et al., 2024):

- *Summer 2014:* Seven of the largest banks in the United States were compromised by four hackers who exploited the Heartbleed vulnerability and distributed advanced malware to infiltrate systems. At JPMorgan alone, the attackers accessed personal data of over 76 million individuals and 7 million businesses, including names, addresses, phone numbers, emails, and internal user-related data.

- March 2016: A hacker group infiltrated the systems of Bangladesh Bank and obtained credentials to execute financial transfers. Nearly 30 fraudulent transfer requests were sent to the Federal Reserve Bank of New York, directing funds from Bangladesh Bank's account to recipients in the Philippines and Sri Lanka. Four of these transfers succeeded, totaling USD 81 million. The fifth was halted due to a typo in the recipient's name.

2.3. Digital banking activities and development trends in Vietnam

Driven by the Fourth Industrial Revolution, digital transformation in banking has accelerated as institutions modernize operations to remain competitive and responsive to rapid technological change. Digital banking, as noted by Skinner (2014) and Sharma & Dubey (2022), represents a model in which core banking activities are carried out on digital platforms, extending far beyond traditional internet banking. It requires strong technological capabilities and the integration of advanced tools such as AI, big data, RegTech, APIs and modern digital infrastructure. In essence, a digital bank functions as a "branchless" institution, operating fully online and providing continuous 24/7 services.

In Vietnam, digital transformation has become a central strategic direction across the banking sector. Banks are simultaneously digitizing customer-facing services and internal processes, adopting technologies such as big data analytics, cloud computing, RPA, AI and blockchain to enhance efficiency and customer experience. Alongside technology investment, core banking systems and IT infrastructure are being upgraded to improve safety, resilience and scalability. Cybersecurity has also become a priority area, given its direct influence on service quality and customer trust.

By the end of 2023, two main models of digital banking development had emerged in Vietnam. The first is the transformation of traditional banks through multi-channel digital platforms, seen at institutions such as BIDV, Vietcombank, Techcombank and MB. The second combines this transformation with the creation of standalone digital banks, exemplified by TPBank's LiveBank and VPBank's digital ecosystems such as Yolo, Cake and VPBank NEO.

2.4. Impacts of cybersecurity risks on digital banking operations in Vietnam

Cybercrime involves illegal activities conducted through intermediary computers in cyberspace. In the banking sector, cybercrimes commonly include illegal access (hacking and cracking) and fraudulent or deceptive activities such as phishing and data theft (Douglas et al., 2000; WALL, 2001).

According to the Asia-Pacific Computer Emergency Response Teams (APCERT), between 2013 and 2022, cyberattacks in Vietnam including phishing, defacement, and malware rose from 6,000 cases in 2013 to a peak of 134,000 in 2016. Although attacks dropped significantly in 2018 (about 10,000 cases) and 2019 (over 5,000), they began to rise again in 2020 and continued increasing in 2022 (APCERT, 2022).

Table 1. Number of cybersecurity incidents in Vietnam (2013-2022)

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Incidents	6,214	19,786	15,177	134,375	13,382	9,666	5,176	11,382	10,774	12,694

Source: APCERT Report

Over 50% of cyberattacks in Vietnam target financial institutions (Vietnam Information Security

Association). Data from the Ministry of Information and Communications shows that in the first half of 2023, over 4,000 fraud reports were filed, with over 95% concerning the banking and finance sector.

The deeper banks engage in digital transformation, the higher the cybersecurity risk and associated financial losses (Phuong & Dien, 2021). According to the Ministry of Public Security's Cybersecurity Department, cybersecurity incidents in 2020 caused losses of around VND 100 billion (~USD 4 million), including one targeted bank that lost VND 44 billion (~USD 1.8 million) to hackers.

Attack methods have become increasingly diverse and sophisticated. These include:

(1) Data theft from banks, customer accounts, and credit card information

(2) Email phishing to steal login credentials

(3) Exploiting security loopholes to gain unauthorized administrative access

(4) Attacking databases and hijacking systems to steal funds

With a young population and a high internet penetration rate, Vietnam is well-positioned to promote digital transformation and digital banking (Thanh & Dung, 2022). However, these advantages also come with considerable challenges, particularly in preventing fraud and scams. These include data breaches, defaced or hacked websites, unauthorized transactions causing asset losses, and scams impersonating bank staff or creating fake websites to defraud customers.

In conclusion, digital banks in Vietnam face significant cybersecurity risks. All three key stakeholders banks, partners, and customers are potential targets for cybercriminals. The increasing frequency and sophistication of cyberattacks on Vietnamese banks underscore the urgent need for effective cybersecurity risk management to protect the development of digital banking in the country.

3. Challenges facing banks in cybersecurity risk management

In the financial sector, cyberattacks are six times more frequent than in other sectors, although the average cost per incident tends to be lower. This is largely attributed to tighter regulatory oversight and stronger governance mechanisms to address cyber risks (Aldasoro et al., 2020). For banks, cybersecurity risk accounts for only 0.2% of total operational losses. However, the frequency of such risks is increasing, and the estimated impact on bank revenues may range from 0.2% to 4.2% (Aldasoro et al., 2020; Bouveret, 2019). These figures emphasize the importance of improved system defense and risk mitigation strategies, although banks still face significant challenges in cybersecurity risk management, including:

Procedural challenges

Many banks have yet to establish synchronized and effective cybersecurity risk management processes. In particular, they lack standardized response scenarios for information security incidents and structured procedures to minimize the negative impacts of cyberattacks. Additionally, processes for assisting customers who suffer cybersecurity breaches are often incomplete, leading to a decline in customer trust in digital banking services.

Technological challenges

Despite efforts to invest in IT infrastructure and promote digital transformation toward a comprehensive and secure digital banking model, such investments remain fragmented and outdated. Many banks still rely on legacy systems that lack advanced features for detecting anomalies and preventing cyber incidents. As a result, cyberattacks on the banking sector, particularly on digital banking platforms, continue to rise.

Moreover, cybersecurity risk also arises from how technology is used by external stakeholders, including vendors and customers. Many of the banks' third-party partners do not prioritize cybersecurity. For example, customers may be targeted through promotional emails or SMS messages sent by outsourced marketing service providers. Additionally, many customers are unaware of the importance of protecting their personal information. Such data can be captured through online transactions and subsequently exploited by cybercriminals.

A common vulnerability is the reuse of identical passwords across multiple online services. This practice creates an entry point for hackers to breach multiple accounts and steal sensitive data (Nguyen et al., 2021). Cybercriminals may also use malware embedded in free software or social media platforms to extract private information and commit online fraud, including the illegal sale and exploitation of stolen data.

Human resource challenges

Cybersecurity risk management is inherently complex. It not only requires technical expertise from involved personnel but also necessitates a deep understanding of information security practices. Although many banks have started appointing high-level officers such as Chief Information Security Officers (CISOs) to oversee cybersecurity matters, there remains a significant shortage of qualified professionals in this field.

As technology evolves, cybersecurity strategies and practices must also adapt to proactively identify and address new threats and vulnerabilities. This requires a strong combination of technical knowledge, regulatory compliance, and a commitment to ongoing development of cybersecurity personnel. The goal is not only to defend against threats but to foster

organizational resilience in a constantly evolving digital environment.

4. Solutions to mitigate cybersecurity risks in digital banking operations in Vietnam

Based on the existing challenges in cybersecurity risk management, this section proposes a set of solutions built around three core pillars Processes, Technology, and People along with associated compliance principles, as follows:

Process-Oriented Solutions for Cybersecurity Risk Management

These solutions emphasize the design and implementation of systematic risk management procedures to help banks identify and assess threats, plan prevention strategies, and prepare effective response mechanisms in case of incidents.

According to a global cybersecurity risk management report by Deloitte, only 42% of surveyed respondents rated their organizations as "effective" or "very effective" in managing cyber risks (APCERT, 2022). The report also highlights several common challenges faced by banks and financial institutions, including:

(i) insufficient budgeting for cybersecurity risk management,

(ii) vulnerabilities in legacy core systems and the difficulty of integrating new security tools,

(iii) legal and regulatory constraints regarding information sharing and the lack of standardized cybersecurity risk management frameworks.

Based on these insights, a cybersecurity risk management process may include the following stages (Thuy et al., 2021):

Step 1: Risk Identification

This step involves:

(i) identifying critical assets (information, data) and prioritizing them;

(ii) identifying potential threats to these assets;

(iii) identifying vulnerabilities that may be exploited by such threats.

Step 2: Risk Impact Assessment

Assessing the likelihood and potential consequences of each risk, including cost implications. This assessment informs management decisions on appropriate risk mitigation strategies.

Step 3: Risk Evaluation and Prioritization

Determining whether each risk falls within the bank's acceptable risk tolerance level. This stage involves describing the severity of each risk to determine the level of action required and prioritizing risks to allocate resources efficiently. A combination of qualitative (e.g., low-medium-high levels) and quantitative (e.g., probabilities and potential losses) methods may be used.

Step 4: Risk Response Strategy

Based on the evaluation, banks may choose to:

(1) Mitigate the risk;

(2) Accept the risk;

(3) Avoid the risk;

(4) Transfer the risk (e.g., via insurance or outsourcing).

Step 5: Risk Monitoring

Regularly reviewing control measures to ensure they remain appropriate in the face of evolving cyber threats.

Technology-Oriented Solutions

Technology plays a crucial role in determining the effectiveness of cybersecurity efforts. The use of advanced technologies enables banks to enhance the efficiency of process implementation and compliance monitoring, reduce the time needed to detect risks, and accelerate response times during incidents. Moreover, automation facilitates real-time reaction and remediation of security breaches.

However, investing in advanced cybersecurity technologies requires significant capital, as well as a synchronized approach to IT infrastructure development. Therefore, banks should evaluate and select technologies based on three key criteria:

(1) speed of threat detection,

(2) speed of incident response,

(3) recovery time.

Accenture Security (2022) emphasizes that effective cybersecurity risk management strategies are built on modern security tools and techniques. Two technologies receiving the highest ratings from global banks for cybersecurity investment are:

- Artificial Intelligence (AI)

- Security Orchestration, Automation, and Response (SOAR)

Although Blockchain is often cited as a promising solution due to its distributed structure, consensus-based verification, encrypted data, and transparency, its application must be approached with caution. This is because the technology still carries unpredictable risks, such as software encryption errors or threats arising from external data sources that may open new attack vectors.

Human-Centered Solutions

Regardless of how advanced a bank's technology or security protocols may be, cybersecurity will always be vulnerable to human factors. Therefore, it is critical to strengthen awareness and foster a cybersecurity culture within the organization through the following measures:

Internal Staff Training

Bank employees serve as the first line of defense against cyber threats. Raising staff awareness about data protection and equipping them with knowledge of common cyber risks is essential. Training programs should cover:

(1) responsibilities related to banking data;

(2) documentation and reporting procedures;

(3) password usage and unauthorized software risks;

(4) safe internet and email practices;

(5) social engineering attacks, online fraud, phishing, and safe web browsing.

Customer Education

Banks should actively promote cybersecurity awareness among customers to help them protect personal information. Training and education can be delivered through multiple channels, such as:

(1) official bank websites;

(2) social media platforms;

(3) alerts and safety tips on account protection. These efforts not only reduce the risk of cyber incidents but also increase customer trust in how the bank safeguards their data.

Compliance with Preventive Principles

In addition to the core pillars, commercial banks must strictly adhere to the following preventive principles to ensure comprehensive cybersecurity protection (Kay et al., 2021):

(1) Employ multi-layered security defenses instead of relying on a single security solution

(2) Perform regular data backups to mitigate losses from data breaches or system failures

(3) Continuously update software and systems to patch security vulnerabilities

(4) Integrate biometric authentication into security protocols

(5) Respond promptly to cyberattacks to minimize damages

(6) Raise awareness among employees and customers regarding cybersecurity threats

(7) Routinely review and update the bank's security strategies

(8) Develop a comprehensive incident response plan for cyberattacks

Lastly, as Vietnamese banks aim to become fully digital in the ongoing transformation process, Pearlson et al. (2020), in their case study of C6 Bank in Brazil, proposed a cybersecurity policy framework for digital banks based on five functional groups:

(1) defense group,

(2) technical group,

(3) governance group,

(4) application safety group, and

(5) cybersecurity culture group.

Additionally, cybersecurity risks should be managed under the three-lines-of-defense model, which includes: the operational process layer, the risk control and compliance assurance layer and the internal audit layer.

5. Conclusion

In the context of accelerating digital technology adoption in the Vietnamese banking sector, cybersecurity risk represents one of the most critical challenges to the transformation and development of digital banking. It is considered a vital issue that significantly influences the success of comprehensive digital transformation across Vietnam's banking system. This paper has provided a comprehensive overview of cybersecurity risks, the current landscape of digital banking development in Vietnam, and an analysis of the impacts of cyber risks on digital banking operations. It has also identified major challenges in cybersecurity risk management currently faced by banks. To mitigate these risks, banks must adopt a comprehensive set of solutions focused on three core pillars: processes, technology and people. Furthermore, to operationalize these solutions effectively, banks need to adhere strictly to cybersecurity risk governance principles while simultaneously building a structured cybersecurity risk management process and cultivating a cybersecurity-aware organizational culture. By doing so, banks will be better positioned to prevent and minimize the threats posed by cybersecurity risks in both general banking activities and digital banking operations in particular within Vietnam.

References:

Aldasoro, I., Frost, J., Gambacorta, L., Leach, T., & Whyte, D. (2020). Cyber risk in the financial sector. SUERF Policy Notes, 206.

Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021). Covid-19 and cyber risk in the financial sector. Retrieved from https://www.bis.org

APCERT. (2022). APCERT annual report. Retrieved from https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2022.pdf

Douglas, T., Thomas, D., & Loader, B. (2000). Cybercrime: Law enforcement, security and surveillance in the information age. Routledge.

IBM. (2023). Cost of data breach report. Retrieved from https://www.ibm.com/reports/data-breach

Kay, A., Hutcherson, C., Keene, C., Zhang, X., & Terwilliger, M. G. (2021). How financial institutions address cybersecurity threats: A critical analysis. Issues in Information Systems, 22(1), 63-74.

Keeper Security. (2020). Nearly 70% of financial services companies globally have experienced a cyberattack. Retrieved from https://keepersecurity.s3.amazonaws.com/press/pdf/2020/May/FinancialServices.pdf

Mundial, F. E. (2020). Global Risk Report 2020. Retrieved from http://reports.weforum.org

Nguyễn, V. M., Nguyễn, T. T. T., & Hà, N. M. (2021). Protecting the legal rights and interests of individual customers against high-tech crime. Journal of Legal Science and Practice (Vietnamese).

Pearlson, K., Li, M., & Chou, S. (2020). Cybersecurity culture at C6 Bank. Retrieved from https://cams.mit.edu/wp-content/uploads/Cybersecurity-Culture-at-C6-Bank-CaseStudy.pdf

Phương, N. V., & Diễn, T. V. (2021). Cybersecurity risks and challenges in the banking sector in Vietnam. Journal of Economics and Business Administration - Ho Chi Minh City Open University, 16(2), 30-44.

Thanh, N. H., & Dũng, N. Đ. (2022). Factors promoting the development of digital banking in Vietnam. Journal of Finance and Accounting Research, 3, 65-68.

Thúy, P. C., Hiền, P. T., & Anh, H. N. Q. (2021). Cybersecurity risks in digital banking operations: The case of Vietnam. Information and Communications Publishing House (Vietnamese).

Trần, H. K., & Nguyễn, T. K. (2021). A review of cyberattack methods in the past decade. Journal of Science and Economic Development, (12), 101-112.