Journal of Business and Future Economy
Vol. 1, No. 1, pp. 57-64
Winter 2024

JBFE

A framework for examining the dimensions and components of cyber security in smart banking

Jon Lendasce[1*]

[1]*University of Colombia, Colombia*

Abstract

Cyber security is one of the most essential elements in banking today. Banks are not only responsible for their customers' assets but may also lose their credibility after a data breach. Unfortunately, banks are one of the biggest targets of cyber-attacks because they hold vast amounts of sensitive customer data that provide potential financial gain to hackers and criminals. Therefore, in the digital economy, cyber security is necessary to protect financial data, and its effectiveness in banks affects the safety of customer information. To improve the customer experience, innovative banking provides services on a digital platform using new technologies such as artificial intelligence. Considering the changes that have taken place and the transition to intelligent banking, it is essential to maintain the security and manage the risks of innovative banking. This article investigates the challenges, benefits, and threats of using intelligent technologies based on security in innovative banking.

Keywords: smart banking, cyber security, information security

1- Introduction

The changes that have occurred in the digital banking sector have led to the emergence of various cyber threats in this industry. According to recent reports, unforeseen cyber threats can completely disrupt the main and key activities of financial departments. Therefore, threat management and network security protocols are very important. Undoubtedly, cyber attackers are looking for financial benefits. As a result, cyber threats are increasing and always moving towards complexity (Aliahmadi et al., 2022).

The management of cyber threats in today's banking space goes beyond technical measures and requires a more comprehensive approach. However, many financial institutions are

* Corresponding author: Lendasce @gmail.com

fighting cyber threats with limited tools, especially when integrating with new digital technologies (Gharachorloo et al., 2021).

Recent regulatory rules in the financial industry emphasize operational flexibility and risk management. This global convergence seeks to standardize approaches and integrate them. One notable aspect of these regulations is increased scrutiny of third-party providers in the financial ecosystem. It should be noted that third-party providers who provide services but are not part of the system have become very important today, and there is an excellent need to assess and manage the associated risks (Bathaee et al., 2023).

Banks have always been cautious in choosing information technology suppliers due to the critical nature of banking operations and the need for reliable and secure solutions. On the other hand, the emergence of startups providing new technologies and services can increase banks' productivity (Nozari et al., 2021). However, these new conditions must be carefully balanced, primarily when the third-party category is raised, because they can cause security vulnerabilities. As banks' digitization evolves, a coordinated approach to risk management that considers global regulations and third-party integration is essential (Mohammadi et al., 2015).

Digital transformation has transformed the banking system. With the digitization of banking services, the role of bank branches is also changing. Banks seek innovative ways to optimize their performance, control inconsistent risks, and improve customer satisfaction in a highly competitive and evolving market. In this regard, with the boom of mobile communication technology and Internet applications, innovative banks emerged to improve offline service capabilities and enhance user experience. These new players seek a competitive advantage by simplifying the account opening process and providing personalized services around the clock. While the challenges facing intelligent banks in security, risk, and operations cannot be ignored, we are now trying to find solutions to overcome the difficulties and strengthen the protection of banks while addressing the challenges in this field (Aliahmadi et al., 2015).

2- Literature review

In the past, banks operated as separate institutions and departments, each of which often had unique goals and operated independently of each other. Such an approach brought several disadvantages for banking, which caused dissatisfaction among customers. This is why traditional banks are known for cumbersome processes and difficulties accessing services or support. Implementing an integrated platform is highly recommended to address these challenges. However, the information placed in separate departments causes the escalation of cyber threats, data breaches, and non-compliance with regulations (Movahed et al., 2024). It takes them beyond operational inefficiency, which is considered a banking challenge today.

Ensuring the security and reliability of the banking IT infrastructure and the vast amount of data it manages is very important, especially as the bank undergoes digital transformation. On the other hand, dealing with technical debt is also very important and emphasized a lot. Technical debt refers to the implicit costs that businesses do not take to fix problems that affect the future. Accumulation of technical debt makes existing problems more severe over time and its compensation costs more. The term debt in this industry refers to modernizing old infrastructure to align with current technologies and standards. To address the challenges

above, banks should consider dedicated units with professional and experienced teams to focus on innovation and remain competitive (Nozari et al., 2024).

The modern banking ecosystem consists of tens or hundreds of thousands of interconnected devices, including computers and IoT devices. At the same time, expanding channels, including social media, cloud services, and mobile applications, have added to its complexity. Each of these channels presents its own set of security challenges. Now, the question arises: How can banks stay safe amid such vast network complexity?

Financial institutions desperately need digital initiatives to stay competitive and meet their customers' evolving needs. These initiatives include using new technology and solutions to improve services and functions. Organizations must quickly adapt to new challenges and threats in the digital field (Nahr et al., 2021).

3- Cyber security in digital banking

As banks increasingly move into the digital space to better serve customers, the need to be proactive in combating cyber security threats is critical. Five of the most important cyber security threats in digital banking are (Nozari et al., 2021):

- Digital currency has become a cyber target for criminals because it is difficult to trace funds lost through hard cryptocurrencies and recover them even with the help of a regulatory body.
- Since businesses have changed to remote work environments in recent years, malware attacks have also increased.
- In digital banking, cloud-based cyber-attacks are on the rise as more applications and data are stored in the cloud.
- Financial institutions are experiencing more severe attacks by using new technologies. For example, the two technologies of machine learning and smart contracts, while they are in the early stages of adoption and still suffer from error codes and weak algorithms, can be exploited by smart hackers.
- Fraud and identity theft have always existed. While these attacks are not new to financial institutions, they are evolving through digital channels. Digital banking has expanded through smart devices. On the other hand, weak passwords, lack of encryption and lost authentication process in mobile phones all increase the security risks of the bank network.
- Older systems are more vulnerable to security threats. These systems often lack proper functionality against digital banking threats. Therefore, organizations that use old systems are at risk of security breaches and data loss.

4- Cyber security challenges

Cyber threats targeting banks are constantly increasing. Banks were attacked an average of 700 times per week in 2020. The specific challenges of smart banks that increase cyber vulnerability include the following (Ghahremani-Nahr et al., 2021):

- Increasing acceptance of new technologies due to digital transformations
- Create hybrid data centers

- Cloud network challenges
- Increasing the use of online and mobile channels to meet banking needs
- The speed of proliferation of Internet of Things devices
- Cyber security related to privacy
- Global shortage of cybersecurity experts
- Cyber risk associated with remote work

One of the biggest challenges faced by smart banks in the field of security is the issue of theft and other forms of threats. While most banks rely on video surveillance of public branches, head offices, critical infrastructure buildings as well as entrances, parking lots, ATM terminals, etc. for security, when investigating and preventing crime with traditional surveillance with They face many challenges (Nozari et al., 2021).

- **Operational challenges**

Replacing the main systems, changing digital business models, redesigning marketing methods and optimizing branch operations in banking are still tricky and can be considered as limiting factors for the establishment of smart banking.

- **Internet of Things devices**

Various devices face problems when using innovative banking applications. The banking, display, security, electrical, and other IoT device protocols differ significantly. Each manufacturer uses a different coding format for Internet of Things devices, which can be challenging when implementing innovative banking. In addition, integrating IoT technologies requires significant financial and technological investments.

The complexity of the Internet of Things system affects both hardware and software. Most of the information processing in Internet of Things systems is done through special-purpose or even general-purpose processors. One of the weaknesses of Internet of Things devices is the intrusion of an attacker or hardware trojan into the system during the chip design or manufacturing process, and this has caused serious concerns for medical, nuclear, banking, and economic systems.

- **Digital customer acquisition**

Today, the Internet is a crucial channel for banks to attract customers. Financial institutions must develop online customer engagement capabilities to understand customers better, reduce risks, and improve customer service.

- **Technology infrastructure**

New technologies that require huge investments define the future of financial services. Creating the technology infrastructure and applying the right strategy in technology selection is as challenging as providing the best solutions to customers.

We are also at risk of technology and service disruptions whenever we use the Internet. System inefficiencies can affect customers' ability to access their accounts if the Internet slows down or stops altogether. System crashes can be challenging as users cannot pay or complete transactions. Additionally, IT system downtime can cost businesses $1.55 million annually.

- **Policies and regulations**

Banks are facing a lack of transparency regarding the regulations of using new technologies. There are no regulations for transfers made with digital currencies and smart contracts. Until an appropriate legal framework is established, it will be challenging for financial institutions to use blockchain. In addition, the rules of the Internet of Things are not limited to geographical boundaries. The lack of a single and global approach to the laws of the Internet of Things creates a potential challenge in using this technology. Discriminatory use of data, use of data for law enforcement, and the issue of data ownership are just three examples of big data challenges that must be overcome in intelligent banking.

5- Cybersecurity frameworks

The Cybersecurity Framework sets out standards that will facilitate the processes and procedures that banks must follow to assess, monitor, and mitigate risk.

The NIST Cybersecurity Framework has emerged as the gold standard for assessing cybersecurity maturity, identifying security vulnerabilities, and adhering to cybersecurity laws.

Figure 1 shows the NIST cybersecurity framework.

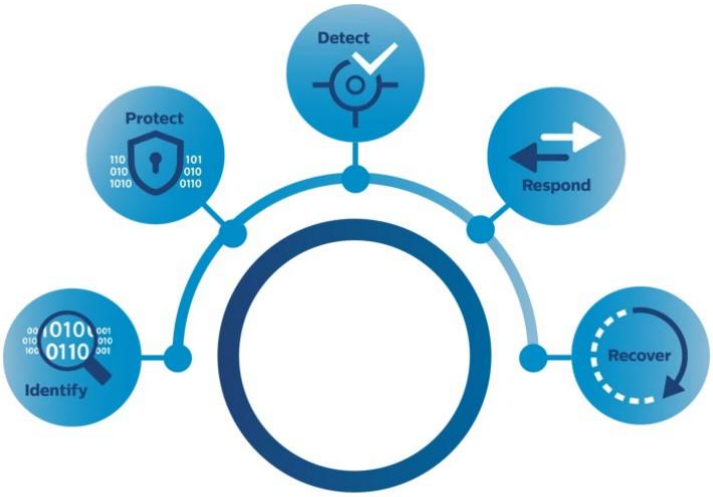

Figure 1: NIST Cybersecurity Framework

Unauthorized access to banking networks will destroy them; Financial losses and banking data breaches may result from phishing attacks. When a victim clicks on a link in a message or email, malicious code from phishing websites is executed on the user's device, and the attacker can gain access to the system while remaining undetected for a long period. Phishing attacks are carried out so that the victim cannot tell whether the email or message is sent from a legitimate source or a hacker.

Smart banking requires open and distributed technologies that support the rapid development and deployment of next-generation applications and data platforms, accelerate

customer acquisition, and enhance the customer experience. In addition, it has reduced IT costs so that banks can quickly rebuild data lakes and data factories. Technology standardization reduces complexity and also improves cost savings through economies of scale, ease of integration, improved efficiency and better IT support. Open banking APIs act as the connective tissue in the smart banking ecosystem, facilitating seamless interactions between different financial platforms and services. They provide a standardized tool for banks and fintech companies to securely share data, ultimately promoting innovation and competition in the industry. Smart banks should be equipped with cloud technology to improve customer service and increase productivity. Using the power of the cloud, banks can automate customer service processes and implement intelligent risk management systems and tailor services to individual needs. Cloud migration is a key component of successful IT infrastructure management. Now, if the main operations remain in the old IT system, there is no point in moving services and peripheral systems to the cloud. The open banking system uses a distributed architecture based on microservices, so that banks can develop extraordinary applications and migrate traditional core systems to new intelligent systems over time. Figure 2 shows the cyber security framework for smart banking.

Figure 2: A framework for cyber security in smart banking

This framework uses information from credible commercial and government sources to identify potential attackers to a specific financial institution. Then, it imitates the methods of these potential attackers to assess the cyber security of banks. In this way, banks identify the weak points of their systems and implement corrective measures.

6- Conclusion

As technology advances, cyber threats also become more sophisticated and advanced. For this reason, banks must constantly update their security strategies and technologies. Investing in research and development of new cyber security technologies and cooperation with fintech

companies can help improve security in this area. Cybersecurity in banking is a critical and complex issue that requires constant attention and investment. With constantly changing and evolving cyber threats, banks must use multi-layered approaches and advanced technologies to protect customer information and assets. Also, training and informing customers and employees can play an essential role in reducing security risks. Cyber security should always be considered a top priority in banks' strategies to maintain customer trust and prevent financial and credit losses.

References

Aliahmadi, A., Nozari, H., Ghahremani-Nahr, J., & Szmelter-Jarosz, A. (2022). Evaluation of key impression of resilient supply chain based on artificial intelligence of things (AIoT). arXiv preprint arXiv:2207.13174.

Aliahmadi, A., Sadeghi, M. E., Nozari, H., Jafari-Eskandari, M., & Najafi, S. E. (2015). Studying key factors to creating competitive advantage in science Park. In Proceedings of the ninth international conference on management science and engineering management (pp. 977-987). Springer Berlin Heidelberg.

Bathaee, M., Nozari, H., & Szmelter-Jarosz, A. (2023). Designing a new location-allocation and routing model with simultaneous pick-up and delivery in a closed-loop supply chain network under uncertainty. Logistics, 7(1), 3.

Ghahremani-Nahr, J., Nozari, H., & Najafi, S. E. (2020). Design a green closed loop supply chain network by considering discount under uncertainty. Journal of applied research on industrial engineering, 7(3), 238-266.

Gharachorloo, N., Nahr, J. G., & Nozari, H. (2021). SWOT analysis in the General Organization of Labor, Cooperation and Social Welfare of East Azerbaijan Province with a scientific and technological approach. International Journal of Innovation in Engineering, 1(4), 47-61.

Mohammadi, H., Ghazanfari, M., Nozari, H., & Shafiezad, O. (2015). Combining the theory of constraints with system dynamics: A general model (case study of the subsidized milk industry). International journal of management science and engineering management, 10(2), 102-108.

Movahed, A. B., Movahed, A. B., & Nozari, H. (2024). Opportunities and Challenges of Marketing 5.0. Smart and Sustainable Interactive Marketing, 1-21.

Nahr, J. G., Nozari, H., & Sadeghi, M. E. (2021). Green supply chain based on artificial intelligence of things (AIoT). International Journal of Innovation in Management, Economics and Social Sciences, 1(2), 56-63.

Nozari, H., & Ghahremani-Nahr, J. (2021). Provide a framework for implementing agile big data-based supply chain (case study: FMCG companies). Innovation management and operational strategies, 2(2), 128-136.

Nozari, H., Fallah, M., & Szmelter-Jarosz, A. (2021). A conceptual framework of green smart IoT-based supply chain management. International journal of research in industrial engineering, 10(1), 22-34.

Nozari, H., Fallah, M., Kazemipoor, H., & Najafi, S. E. (2021). Big data analysis of IoT-based supply chain management considering FMCG industries. Бизнес-информатика, 15(1 (eng)), 78-96.

Nozari, H., Szmelter-Jarosz, A., & Ghahremani-Nahr, J. (2021). The ideas of sustainable and green marketing based on the internet of everything—the case of the dairy industry. Future Internet, 13(10), 266.

Nozari, H., Szmelter-Jarosz, A., & Ghahremani-Nahr, J. (2022). Analysis of the challenges of artificial intelligence of things (AIoT) for the smart supply chain (case study: FMCG industries). Sensors, 22(8), 2931.

Nozari, H., Tavakkoli-Moghaddam, R., & Dolgui, A. (2024, September). Analysis of Critical Success Factors of Sustainable and Resilient Aioe-based Supply Chain in Industry 5.0. In IFIP International Conference on Advances in Production Management Systems (pp. 76-90). Cham: Springer Nature Switzerland.