Cybersecurity in Financial Services

Matthew Nojimu Olanipekun Sadiku [1], **Samuel Abiola Ajayi** [2], **Janet Oluyinka Sadiku** [3]

[1] *Prairie View A&M University*
700 University Drive, Prairie View, Texas 77446, USA

[2] *Texas Southern University*
3100 Cleburne Street, Houston, TX 77004, USA

[3] *Juliana King University*
6464 Savoy Drive, Suite 440, Houston, Texas 77036, USA

DOI: 10.22178/pos.116-21

JEL Classification: K39

Received 25.03.2025
Accepted 25.04.2025
Published online 30.04.2025

Corresponding Author:
Samuel Abiola Ajayi
ajayisamuel645@gmail.com

Abstract. Financial institutions handle a lot of money and sensitive data, making them an attractive target for cybercriminals. The safety of digital financial assets makes the finance industry very vulnerable to cyber-attacks. Banks, investment, and insurance firms are always pleasing to cybercriminals with increasingly evolving attack methods. From ransomware attacks to insider threats, the risks are diverse and ever-evolving. Cybersecurity in the financial industry refers to the practices, technologies, and processes used to protect financial institutions (such as banks, credit unions and investment companies), their customers, and their assets from cyber threats. It is an essential component of modern financial services delivery. It is a high-stakes challenge that demands constant vigilance and innovation. This paper explores the critical role of cybersecurity in the finance industry.

Keywords: security, cybersecurity, finance, banking, finance industry.

INTRODUCTION

Financial services encompass many businesses that manage money, including credit unions, banks, credit card companies, insurance companies, consumer finance companies, stock brokerages, investment funds, and some government-sponsored enterprises. These institutions play a critical role in the global economy. The digital transformation has made financial services more accessible and convenient. Although digitalising financial services has brought various benefits, it has also raised the stakes concerning cybersecurity. Financial cybersecurity is a critical issue for enterprises today. Cyber threats to global financial systems could seriously disrupt financial systems, including necessary financial infrastructure, leading to broader financial stability implications. Figure 1 shows the cloud word for cybersecurity.

The financial services industry is one of the most targeted industries for cyberattacks because financial institutions store much personally identifiable information, including social security numbers, account details, and credit card information, making them a goldmine for cybercriminals. Cyberattacks targeting financial institutions are becoming more sophisticated, with attackers employing techniques such as phishing, ransomware, and insider threats. Cybercriminals exploit vulnerabilities in authentication systems to carry out fraudulent transactions or steal customer identities, leading to significant financial and reputational damage [2].

Figure 1 – Cloud word for cybersecurity [1]

RESULTS AND DISCUSSION

Overview of cybersecurity. Cybersecurity refers to technologies and practices that protect networks and information from damage or unauthorised access. It is vital because governments, companies, and military organisations collect, process, and store a lot of data. As shown in Figure 2, cybersecurity involves multiple issues related to people, processes, and technology [3].

Figure 2 – Cybersecurity involves multiple issues related to people, processes, and technology [3]

Figure 3 shows different components of cybersecurity [4].

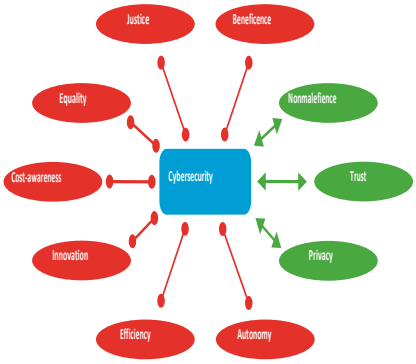

Figure 3 – Different components of cybersecurity [4]
Notes: Green – supportive; red – in tension

A typical cyber-attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cybercriminals or ethical hackers are modern-day digital warriors possessing extraordinary skills and knowledge to breach even the most impregnable systems. A typical cybercriminal is shown in Figure 4. Cyber-attacks are becoming more frequent, sophisticated, dangerous, and destructive.

Figure 4 – A typical cybercriminal [5]

They threaten the operation of businesses, banks, companies, and government networks. They vary from crimes committed by individual citizens (hacking) to actions committed by groups (terrorists) [6].

Cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [7]. These are known as the pillars of information assurance.

Availability: This refers to the availability of information and ensuring that authorised parties can access the information when needed. Attacks targeting the availability of service generally lead to denial of service.

Authenticity: This ensures that the identity of an individual user or system is the identity claimed; this usually involves using a username and password to validate the user's identity. It may also take the form of what you have, such as a driver's license, an RSA token, or a smart card.

Integrity: Data integrity means information is authentic and complete; this assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When attackers target integrity, they also compromise nonrepudiation.

Confidentiality: Ensures that organisations prevent sensitive information from reaching the wrong persons. Data secrecy is essential, especially for privacy-sensitive data such as user personal information and meter readings.

Nonrepudiation: This is an assurance of the responsibility for an action. The source should not be able to deny sending a message, while the destination should not deny receiving it. This security objective is essential for accountability and liability.

Good cybersecurity practices in construction companies should include all of these elements.

Everybody is at risk of a cyber attack. Cyber attacks vary from the crime of individual citizens (hacking) to the actions of groups (terrorists). The following are typical examples of cyber attacks or threats [8]:

Malware: This malicious software or code includes traditional computer viruses, worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is malware that collects information without the victim's knowledge.

Phishing: Criminals trick victims into handing over their personal information, such as online passwords, social security numbers, and credit card numbers.

Denial-of-Service Attacks: These are designed to make a network resource unavailable to its intended users. These can prevent users from accessing email, websites, online accounts or other services.

Social Engineering Attacks: A cybercriminal attempts to trick users into disclosing sensitive information. A social engineer aims to convince a user to disclose secrets such as passwords, card numbers, or social security numbers through impersonation.

Man-In-the-Middle Attack: This is a cyber attack where a malicious attacker secretly inserts themself into a conversation between two parties who believe they are directly communicating. A typical example of a man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

Figure 5 illustrates these and other cyber attacks or threats. Figure 6 displays the sources of cybersecurity threats.

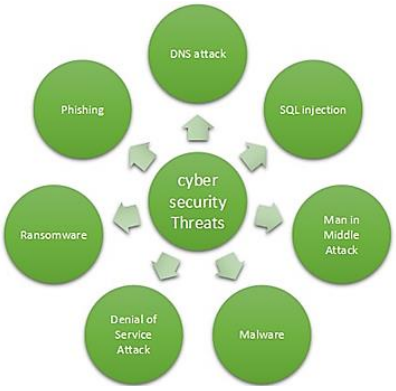

Figure 5 – Common types of cybersecurity threats [9]

Figure 6 – Sources of cybersecurity threats [10]

Businesses, organisations, and governments increasingly recognise cybersecurity's social and financial importance. Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [11]. Cybersecurity is the joint responsibility of all relevant stakeholders, including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organisations play a key role in cybersecurity issues. Securing cyberspace is a high priority for the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron, Skycure, Lookout, and Wandera.

Cybersecurity in Financial Services. The financial services industry includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organisations, and critical financial utilities and services that support these functions.

The industry handles a vast amount of sensitive data, including their customers' personal and fi-

nancial information; this makes financial institutions a prime target for hackers and cybercriminals who want to steal that data. To fight back, financial services companies need to beef up their approach to cybersecurity.

As financial services companies around the world race to keep pace with a rapidly evolving technology landscape, they should consider not only what benefits new emerging technologies offer but also what risks they introduce. While these technologies can provide exponential benefits, they can also bring cyber risks that companies must mitigate using their existing cybersecurity capabilities. Financial services companies must rely upon their foundational cybersecurity capabilities to secure their technologies and protect their environments.

Cybersecurity is more than just a technical imperative; it is also a requirement for maintaining Trust and integrity within the financial system. Financial institutions possess a vast amount of sensitive customer data, including personal information, account information, and transaction details. This information is prone to theft and hacking if there is no cybersecurity. Cyberattacks can result in significant financial losses through fraud or theft, including the loss of services. Cybersecurity in the financial sector involves all the measures aimed at digital asset protection, customer information, and business operations from cyberattacks. In carrying out their activities, cybercriminals take advantage of what drives financial services companies – their customers' Trust, integrity, and credibility [12].

Security finance, often called financial cybersecurity, protects financial institutions and their clients from cyber threats. Financial services cybersecurity is essential for preventing banking cyber-attacks and ensuring the security of online and mobile banking platforms.

Today, nearly all transactions can be conducted online via a bank's mobile application or website, making data security in the banking industry a critical concern. Cybersecurity in the banking sector refers to the measures and technologies employed by financial institutions to protect against unauthorised access, cyber threats, and data breaches. The main objective and importance of cybersecurity in banking is protecting the user's assets. Strong cybersecurity in the banking industry is vital to safeguard sensitive financial data and prevent scam activity. Cybersecurity ensures data integrity and economic stability for banks and their customers [13]. Figure 7 shows some cybersecurity threats in banking.

Figure 7 – Some cybersecurity threats in banking [14]

Combating cybersecurity in financial services

Combating cybercrime demands a united response. All financial institutions, government agencies, and cybersecurity firms collaborate to build a more resilient financial ecosystem. There are several ways to protect financial organisations effectively, such as establishing a robust security posture. The most common and widely used methods by financial organisations to protect against cyber attacks include the following [15]:

Multi-Factor Authentication: Multi-factor authentication (MFA) requires individuals to verify themselves in multiple ways before accessing sensitive systems or data. The method gives an added level of security beyond just passwords, thus making unauthorised access to the financial system significantly more difficult. MFA serves as an additional security measure for online and mobile banking. Beyond just a password, MFA necessitates another confirmation step, such as a code received on your phone or a fingerprint scan.

Employee Education: As technology advances and threat actors become more adept, businesses must adopt a proactive cybersecurity approach. One of the fundamental pillars of this approach is data literacy and education, equipping employees and stakeholders with the knowledge and skills to understand, interpret, and protect data effectively. Train employees on cyber threats, safe best practices online, and the significance of data protection. Through constant employee training sessions, it becomes easy to recognise some cyber threats and enhance employee

awareness about their roles in ensuring the organisation's cyber security. Figure 8 shows why we need cybersecurity training.

Figure 8 – Why we need cybersecurity training [10]

Encrypt Sensitive Data: Data, whether at rest or in transit, using strong encryption protocols, will ensure that even though it is intercepted or stolen, it will remain unreadable and unusable to the unauthorised entity.

Quantum-Resistant Cryptography: With the advent of quantum computing, traditional cryptographic methods could become vulnerable to attacks. Implementing quantum-resistant cryptography ensures data remains secure against future quantum threats.

Incident Response Plan: Establish and review an enterprise-wide incident response strategy to help reduce the risk of cyber incidents, including definitional response activities required to mitigate the threat, minimise damage, and restore systems to operational status following an actual or suspected attack.

Regular Risk Assessment: Your organisation's cybersecurity processes should regularly assess the risks. This best practice will help identify potential vulnerabilities, review the quality of existing security measures, and prioritise areas that need improvement in your security strategy.

Continuous Monitoring: It uses an advanced monitoring tool set with threat intelligence feeds to detect threats as early as possible; this helps in the fast identification of security incidents and quick rectification before they spread.

Zero Trust Architecture: Zero Trust is a core principle of cybersecurity in the financial sector. It assumes that every user, device, and network is potentially compromised and requires authentication and verification at every step. Zero Trust is a security model that assumes no user or device should be inherently trusted. Instead, access is verified continuously based on various factors. With a Zero Trust architecture, you reduce risk by following three core principles: never trust anyone until verified, assume that a breach has already occurred or is inevitable, and apply for least privileged access by only granting minimum privileges to perform the job. Implementing Zero trust architecture can significantly reduce the risk of lateral movement within networks and minimise the impact of potential breaches.

Benefits. With attacks growing more dangerous and frequent, security leaders in finance are doubling down on their efforts to protect their organisations. The financial sector is one of the most regulated and mature industries in terms of cybersecurity. Cybersecurity for financial services is instrumental in preventing losses. Financial institutions, such as banks, investment firms, and insurance companies, are responsible for the security and privacy of the vast amounts of personal and financial data entrusted to them. Other benefits include the following:

Enhancing Efficiency: Strong cybersecurity practices protect financial institutions from cyberattacks and improve operational efficiency. When systems and data are secured, institutions can ensure uninterrupted services and minimise downtime caused by cyber incidents; this is crucial for maintaining customer satisfaction and confidence.

Reputation Protection: Trust and credibility are the two most essential objectives for people when choosing a particular provider for financial services. A successful cyberattack would likely cause irreparable damage to the reputation of any financial institution through loss of customers' Trust and a reduction in business opportunities. Good cybersecurity protects data while showing a commitment to maintaining stakeholders' interests.

Mitigating Risks: Cyberattacks on financial firms have become a flourishing money-making business for cybercriminals. Implementing robust cybersecurity solutions can help financial institutions reduce cyber risks in the constantly developing world of cyber threats. Implementing a cybersecurity framework in banking and other financial institutions has become prominent in preventing possible occurrences of cyberattacks. Two significant aspects exist to mitigate cyber

threats to banking and financial institutions. One aspect is email security, and another is employee awareness.

Government Regulations: On a global scale, governments enact laws requiring banks to implement specific cybersecurity practices. These regulations can dictate various aspects of data security, including what needs to be protected, how to handle breaches, and how personally identifiable information is safeguarded.

Challenges. Building and maintaining robust security systems is expensive since it involves a lot of investment in the latest technology and professionals specialising in such matters. The use of AI in cybersecurity raises ethical concerns related to privacy and the potential for misuse. Financial institutions must ensure that their AI systems are used responsibly and transparently. Other challenges include the following [16,17]:

Complexity: Cyber threats are increasing in volume and complexity. Cybersecurity in financial services is a complex picture. Not only has a range of new tech hit the industry in the last five years, but compliance requirements introduce another layer of difficulty to the lives of infosec teams in this sector. As the cyber threats increase in complexity, it will make the security of the sensitive data and information of finance organisations all the more difficult.

Collaboration: Collaboration between financial institutions, technology providers, and regulatory bodies will be essential in creating unified defences against cyber threats. Cooperation and information sharing in cybersecurity empower financial institutions to detect threats faster through interaction, build robust protections, and set a more solid defence against cyber attacks. In the face of increasingly sophisticated cyber threats, collaboration and information sharing among organisations become crucial.

Knowledge Gap: The cybersecurity knowledge gap among employees is a significant risk for financial institutions, stemming from factors such as motivation, behaviours, technology use, and generational differences. Addressing this risk requires motivating employees to keep cybersecurity in mind, fostering safe behaviours, and ensuring effective technology use. Investing in engaging cybersecurity training and promoting a shared responsibility environment is essential for financial institutions to protect against evolving threats.

Standardisation: Beyond general regulations, financial institutions face additional cybersecurity guidelines. These detailed standards, often created by industry groups in collaboration with regulators, outline specific technical controls, risk management strategies, and how to respond to security incidents. A key to enhanced security for emerging and critical technologies is to develop standards on how current cybersecurity and information security measures integrate into the use of these technologies. Tighter integration between these standards and current cyber frameworks will create uniformity in how these technologies are implemented between financial institutions and the agreed security measures for these technology uses.

Regulatory Compliance: Regulators are actively attempting to curb damage due to cyberattacks. Regulators at the state, federal, and international levels have responded to the growth in financial services cyberattacks by implementing new rules for the financial services institutions they supervise. Companies should approach compliance as the minimum baseline of expectations rather than the aspirational goal. Financial institutions operate within a stringent regulatory environment that sets guidelines to ensure the security and integrity of economic systems and protect consumers. Ensuring cybersecurity helps organisations meet standards by avoiding fines and other legal ramifications. Robust cybersecurity measures ensure that an organisation meets the stringent regulatory requirements of the financial industry, thus escaping heavy fines and legal implications.

Consumer Trust: Trust is critical for financial services institutions. Customers entrust their money and personal data to financial institutions, expecting them to keep it safe. Customers must trust that their financial information is secure and that their transactions are conducted safely. Maintaining that Trust has never been more challenging, particularly given the ongoing expansion and growing sophistication of cybercrime and cybercriminals. Any breach of this Trust, such as a data breach or a successful cyber attack, can severely damage a financial institution's reputation and customer relationships. By investing in strong cybersecurity measures, financial institutions can assure their customers that their data is safe, thereby maintaining and even enhancing consumer trust.

Customer Detriment: When a customer suffers a loss due to credit card theft, it is usually possible to recover it from the bank. However, it takes time to recover the finances in cases such as data violations, which is very concerning for customers. Every bank must implement cybersecurity methods to protect its customers' data.

Fraud Prevention: Fraud is consistently a challenge for all financial institutions. Fraud prevention is a top cybersecurity challenge. Although financial services as an industry face many challenges similar to other verticals in cybersecurity, fraud remains unique to the financial services sector, along with the sensitivity of data and its compliance/regulatory requirements. Regulated financial institutions must report to authorities on fraud and financial crime, a key component that regulatory bodies will scrutinise.

CONCLUSIONS

The financial industry is a prime target for cybercriminals due to its high volume of valuable financial data and assets. Cybersecurity is critical to the financial industry's success, protecting sensitive customer data, ensuring the integrity of financial transactions, and confirming compliance with regulatory requirements. It is not a one-off thing but rather an ongoing process during which organisations must remain vigilant. Cyber incidents are increasing in both frequency and severity year over year, and institutions must stay vigilant in their capabilities to defend themselves and protect their assets and finances against electronic crime.

The security practices of financial institutions have evolved. The security landscape is changing in various practices like data security, application security, API security, network security, endpoint security, security monitoring, and cloud security. As the technology landscape in the financial services sector continues to evolve rapidly and the associated risks mount, now is the time to future-proof the environment. Financial institutions must understand the need to be cyber resilient and strive to instil cybersecurity within the organisation's culture [18]. Rapid technological advancements and the evolving cyber landscape shape the future of cybersecurity threats. The books [19-29] provide more information on cybersecurity in the financial services industry.

REFERENCES

1. Cybriant. (2022). *Financial Cybersecurity: Are Banks Doing Enough to Protect You?* Retrieved from https://cybriant.com/2022/10/24/financial-cybersecurity-are-banks-doing-enough-to-protect-you/

2. LinkedIn. (2025). *Cybersecurity Challenges in Financial Services*. Retrieved from https://www.linkedin.com/pulse/cybersecurity-challenges-financial-services-decentcybersecurity-djg8c/

3. Singh, P. (2021). *A layered approach to cybersecurity: People, processes, and technology- explored & explained*. Retrieved from https://www.linkedin.com/pulse/layered-approach-cybersecurity-people-processes-singh-casp-cisc-ces

4. Loi, M., Christen, M., Kleine, N., & Weber, K. (2019). Cybersecurity in health – disentangling value tensions. *Journal of Information Communication and Ethics in Society, 17*(2), 229–245. doi: 10.1108/jices-12-2018-0095

5. Adams, M. (2023). *Unlocking the benefits of ethical hacking: The importance of ethical hackers in cybersecurity*. Retrieved from https://www.businesstechweekly.com/cybersecurity/network-security/ethical-hacking/

6. Sadiku, M. N. O., Alam, S., Sarhan M. Musa, S. M., & Akujuobi, C. M. (2017). A Primer on Cybersecurity. *International Journal of Advances in Scientific Research and Engineering, 3*(8).

7. Sadiku, M. N. O., Tembely, M., & Musa, S. M. (2016). Smart grid cybersecurity. *Journal of Multidisciplinary Engineering Science and Technology, 3*(9)

8. FCC. (2013). *Small Biz Cyber Planning Guide*. Retrieved from https://transition.fcc.gov/cyber/cyberplanner.pdf

9. Infologo. (2025). *The top 8 cyber attacks to watch out for*. Retrieved from https://infologo.ch/en/blog/les-8-principales-cyberattaques-a-surveiller-2/

10. Samociuk, D. (2023). *Cybersecurity in the financial sector: how to prevent potential threats?* Retrieved from https://www.future-processing.com/blog/cybersecurity-in-the-financial-sector-how-to-prevent-potential-threats/

11. Zhang, Y. (2015). Cybersecurity and Reliability of Electric Power Grids in an Interdependent Cyber-Physical Environment (Thesis; University of Toledo).

12. Financial Services. (n. d.). Why Cybercriminals Target Financial Services. Retrieved from https://www.paloaltonetworks.com/industry/unit42-financial-services

13. Nesterenko, A. (2024). *Banking cybersecurity challenges: Safeguarding financial institutions in 2025*. Retrieved from https://dashdevs.com/blog/cybersecurity-in-banking-main-threats-and-challenges-in-2023/

14. Sasovets, I., & Teres, K. (2025). *Cyber Security in Banking: How We Address Rising Challenges*. Retrieved from https://www.techmagic.co/blog/cybersecurity-in-banking

15. SentinelOne. (2025). *Cyber Security in Finance: Key Threats and Strategies*. Retrieved from https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-in-finance/

16. Imperva. (n. d.). Financial Services Cybersecurity. Retrieved from https://www.imperva.com/learn/data-security/financial-services-cybersecurity/

17. Benton, P. (2024). *State of play: cybersecurity in financial services*. Retrieved from https://www.fintechfutures.com/cybersecurity/state-of-play-cybersecurity-in-financial-services

18. Wipro. (2019). *Cybersecurity in the financial sector*. Retrieved from https://www.wipro.com/applications/ready-for-combat-cybersecurity-in-the-financial-sector/

19. Sadiku, M. N. O. (2023). *Cybersecurity and its Applications*. Lap Lambert Academic Publishing.

20. Ozkaya, E., & Aslaner, M. (2019). *Hands-On Cybersecurity for Finance: Identify vulnerabilities and secure your financial services from security breaches*. Packt Publishing.

21. Tatto, A. C. (2024). *Cybersecurity in Finance: Protecting Financial Data and Systems*. Independently Published.

22. Werrell, L. (2023). *Cybersecurity Compliance in UK Financial Services: A Step-by-Step Guide for Compliance Managers.* Kindle Edition.

23. Bouyon, S., & Krause, S. (2018). *Cybersecurity in Finance: Getting the Policy Mix Right.* Centre for European Policy Studies.

24. Lessambo, F. I. (2023). *Anti-Money Laundering, Counter Financing Terrorism and Cybersecurity in the Banking Industry: A Comparative Study within the G-20 (Palgrave Macmillan Studies in Banking and Financial Institutions).* Palgrave Macmillan.

25. Tinazzi, E. (2023). *CyberSecurity: In The Modern Financial Age.* Independently Published.

26. Pomerleau, P., & Lowery, D. L. (2020). Countering cyber threats to financial institutions. In *Springer eBooks*. doi: 10.1007/978-3-030-54054-8

27. Bouveret, A. (2018). Cyber risk for the Financial sector: A framework for Quantitative assessment. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3203026

28. Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends (Future of Business and Finance). Springer.

29. Sadiku, M. N. O., Ajayi, S. A., & Sadiku, J. O. (2025). Artificial Intelligence in Finance. *International Journal of Trend in Research and Development, 12*(2).