World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

CYBERSECURITY RISKS IN OPEN BANKING SYSTEMS: THREATS, VULNERABILITIES, AND MITIGATION STRATEGIES

Tomilola Ayeni *

University of Northampton, Northampton, United Kingdom.
* Corresponding Author

World Journal of Advanced Research and Reviews, 2026, 31(03), 783–785

Publication history: Received on 28 July 2026; revised on 02 September 2026; accepted on 05 September 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.31.3.2300

ABSTRACT

Open banking enables secure data sharing through application programming interfaces, driving innovation in financial services. However, this model introduces cybersecurity risks, including API vulnerabilities, data breaches, and third-party exposure. This paper reviews existing literature on these risks and examines mitigation strategies. Evidence indicates that strong authentication, encryption, regulatory compliance, and continuous monitoring improve system security. The study highlights the importance of standardized protocols and collaborative governance in ensuring secure open banking ecosystems.

Keywords: Open Banking, Cybersecurity, APIs, Financial Technology, Data Protection

1 INTRODUCTION

Open banking has transformed financial services by allowing consumers to share account data with third-party providers to access new services. Regulatory frameworks, such as the Revised Payment Services Directive (PSD2) in Europe, have facilitated open banking adoption by mandating secure API access[1]. While open banking promotes innovation, it significantly expands the attack surface for cyber threats, requiring robust security strategies[2].

2 API VULNERABILITIES

APIs form the backbone of open banking systems. They enable communication between financial institutions and third-party applications but introduce security risks if improperly configured. Weak authentication mechanisms, improper input validation, and lack of rate limiting create potential attack vectors[3]. The Open Web Application Security Project (OWASP) identifies broken object-level authorization and excessive data exposure as critical API vulnerabilities[4]. Failure to secure APIs can result in unauthorized access to sensitive financial data, leading to financial loss and reputational damage[5].

2.1 Data Breaches and Encryption

Data breaches represent a major risk in open banking. The exchange of financial data across multiple platforms increases exposure to cyberattacks. IBM's 2022 Cost of a Data Breach Report indicates that financial institutions experience higher-than-average breach costs[6]. Encryption of data at rest and in transit is essential, but it must be paired

with secure key management practices to ensure effectiveness[7]. Without proper encryption and monitoring, stolen data can be exploited for fraud, identity theft, or unauthorized transactions[8].

Furthermore, Third-party providers are essential for open banking ecosystems but introduce additional vulnerabilities. Providers vary in security maturity, and a single weak link can compromise the entire system[9]. Studies highlight the importance of rigorous vetting processes, continuous security monitoring, and contractual requirements for third-party cybersecurity compliance[10]. Supply chain attacks demonstrate how vulnerabilities in third-party systems can be leveraged to infiltrate larger networks[11].

It is important to note that strong authentication and authorization mechanisms are critical in reducing unauthorized access risks. PSD2 mandates multi-factor authentication, including one-time passwords, biometrics, or security tokens[12]. Behavioral analytics can enhance security by monitoring anomalies in user behavior, which may indicate potential attacks or fraud[13]. Implementing these controls requires balancing security with user experience, as overly complex authentication can lead to decreased adoption or circumvention[12].

3 REGULATORY FRAMEWORKS

Regulatory frameworks such as PSD2 in Europe and local open banking guidelines in other regions provide minimum security standards[14]. However, implementation differences may create uneven protection levels, requiring institutions to exceed regulatory baselines for optimal security[15]. Coordination between regulators and financial institutions is critical to ensuring consistent implementation and compliance across jurisdictions[14].

3.1 Threat Detection and Incident Response

Cybersecurity in open banking is enhanced by continuous monitoring, threat intelligence, and rapid incident response. Machine learning and artificial intelligence can detect anomalies in API usage patterns or transaction behavior[13]. Institutions must implement clear incident response plans, conduct regular testing, and engage in threat intelligence sharing to mitigate the impact of security events[15].

4 CONCLUSION

Despite mitigation strategies, open banking systems face ongoing challenges. Emerging threats and technological advancements necessitate continuous adaptation of security practices. Interoperability requirements can conflict with security measures, creating trade-offs between accessibility and protection[14]. Smaller financial institutions may struggle to implement advanced security controls due to cost constraints, yet proactive investment in cybersecurity often outweighs the financial and reputational costs of a breach[6].

Collaboration among stakeholders is vital. Financial institutions, regulators, and technology providers must establish best practices and share threat intelligence to improve system resilience[14]. Multi-layered security strategies, combining encryption, authentication, monitoring, and governance measures, are necessary to address complex threats in open banking systems[15]. Open banking offers innovation and convenience but introduces significant cybersecurity risks. Effective mitigation requires technical controls, regulatory compliance, and coordinated organizational measures. Strong authentication, encryption, third-party risk management, and behavioral monitoring enhance system security. Continuous oversight, standardized protocols, and stakeholder collaboration are critical to creating secure, resilient open banking ecosystems.

REFERENCES

[1] Zachariadis M, Ozcan P. The API Economy and Digital Transformation in Financial Services. SWIFT Institute; 2017.

[2] Bouveret A. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Paper WP/18/143; 2018.

[3] Gonzalez-Granadillo G, Diaz R, Garcia-Alfaro J. Security of APIs in Open Banking. Computers & Security. 2021;105:102239.

[4] OWASP. API Security Top 10. Open Web Application Security Project; 2023.

[5] IBM Security. Cost of a Data Breach Report. IBM Security; 2022.

[6] NIST. Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology; 2018.

[7] ISO/IEC 27001. Information Security Management Systems. ISO; 2013.

[8] ENISA. Threat Landscape for Financial Sector. European Union Agency for Cybersecurity; 2020.

[9] European Banking Authority. Regulatory Technical Standards on Strong Customer Authentication. EBA; 2019.

[10] UK Open Banking Implementation Entity. Open Banking Security Profile. 2020.

[11] KPMG. Open Banking: Managing Security and Risk. 2021.

[12] Deloitte. Open Banking and Cybersecurity Risks. 2020.

[13] Ahmed M, Mahmood A, Hu J. A Survey of Network Anomaly Detection Techniques. J Netw Comput Appl. 2016;60:19–31.

[14] Financial Stability Board. Effective Practices for Cyber Incident Response. 2020.

[15] Basel Committee on Banking Supervision. Cyber-resilience: Range of Practices. 2018.