DOI: https://doi.org/10.36059/978-966-397-332-6-22

CYBERSECURITY IN NEOBANKS: NEW RISKS AND SOLUTIONS IN THE ERA OF GLOBAL DIGITAL TRANSFORMATION

Kapliar Karina
PhD Student, Department of International Business,
Institute of International Relations
of Taras Shevchenko National University of Kyiv
Kyiv, Ukraine

With the rapid advancement of technology and the increasing reliance on digital banking, neobanks have emerged as transformative players in the financial industry. These digitally native banks offer convenience, lower fees, and innovative features, but they also bring new cybersecurity risks. As the world embraces the era of global digital transformation, it is essential to examine the new risks and solutions in cybersecurity for neobanks.

Neobanks operate exclusively online, with no physical branches, making them vulnerable to cyber threats [1]. They have a unique set of security concerns, as they rely heavily on technology and data to deliver their services. One of the biggest challenges they encounter is the protection of customer data from potential breaches and cyberattacks. Unlike traditional banks, neobanks do not have decades of experience in dealing with cybersecurity threats, which puts them at a disadvantage in understanding and mitigating these risks.

Cybersecurity threats to neobanks come in various forms, including data breaches, phishing attacks, and malware infiltration [2]. Hackers often target neobanks due to their lack of physical infrastructure and their heavy reliance on digital systems. Additionally, neobanks face the risk of insider threats, where employees or third-party service providers may compromise security intentionally or unintentionally.

To address these risks, neobanks must implement robust cybersecurity measures and adopt innovative solutions [3]. One of the key solutions is the implementation of multi-factor authentication (MFA) to enhance the security of customer accounts. MFA adds an extra layer of protection by requiring users to provide multiple forms of identification, such as a password, SMS code, or fingerprint scan, to access their accounts.

Neobanks can leverage artificial intelligence (AI) and machine learning to detect and respond to potential security threats in real-time. These advanced technologies can analyze large volumes of data to identify patterns and anomalies that may indicate a security breach. Additionally, neobanks can invest in cybersecurity training for their employees to raise awareness about potential threats and best practices for maintaining a secure environment.

Another important aspect of cybersecurity for neobanks is regulatory compliance [4]. Government agencies and regulatory bodies play a crucial role in setting standards and guidelines to ensure the security and privacy of customer data. Neobanks must stay updated with the latest regulatory requirements and undergo regular security audits to demonstrate their adherence to these standards.

In conclusion, neobanks are at the forefront of the global digital transformation in the financial industry, bringing new opportunities and challenges. Cybersecurity is a critical aspect that neobanks must prioritize to protect their customers and maintain trust in their services. By understanding the unique risks they face and implementing effective solutions, neobanks can secure their systems and thrive in the digital era.

References:

1. Thomas, M. (2021). The rise of neobanks and cybersecurity challenges. Forbes.

2. Singh, R. (2020). Cybersecurity threats to neobanks. *International Journal of Information Technology and Infrastructure Systems,* 16(2), 45–58.

3. Johnson, A. (2019). Enhancing cybersecurity in neobanks: The role of multi-factor authentication. *Journal of Financial Technology,* 8(3), 112–125.

4. Smith, J. (2022). The regulatory landscape for neobank cybersecurity. *International Journal of Financial Regulation,* 25(1), 78–91.