sciendo

Proceedings of the 6th International Conference on Economics and Social Sciences (2023), ISSN 2704-6524, pp. 710-719

The 6th International Conference on Economics and Social Sciences
Geopolitical Perspectives and Technological Challenges for Sustainable Growth in the 21st Century
June 15-16, 2023
Bucharest University of Economic Studies, Romania

The Impact of Digitalisation and Cyber Risks on the Banking Sector

Eugen-Marian VIERESCU[1], Cătălina Ioana TOADER[2*]

DOI: 10.24789788367405546-066

Abstract

The banking sector has been permanently changed by digitalisation, which transformed banks into more efficient, cost saving, and customer friendly organisations. But this process of transformation and evolution has brought a new threat to the attention of the risk officers, namely the cyber risks, which materialise through data breaches, phishing attacks, or malware. In order to mitigate the consequences, which can be severe, ranging from financial losses to reputational damage and loss of customer trust, it is essential that the banking sector has in place effective cyber risk management. This paper analyses the relationship between digitalisation and cyber threats in the banking industry, presents the challenges of managing these risks, and provides recommendations for banks to improve their risk management practices. The results suggest that banks should have in place integrated cyber risk management policies, with strategic pillars such as regular risk assessments, employee training, and the implementation of the latest security technologies.

Keywords: risk management, cyber risks, digitalisation, banks.

JEL Classification: G21, G32.

1. Introduction

The use of digital technologies has brought significant changes to the banking sector, leading to increased efficiency, cost savings, and improved customer experiences. However, these benefits have come with new risks, particularly in the form of cyber threats that can result in significant financial and reputational losses for banks. Cyber threats in the banking sector can come in different forms, including data breaches, phishing attacks, malware, and insider threats. These threats have

[1] Bucharest University of Economic Studies, Bucharest, Romania, vierescueugen@gmail.com.
[2] Bucharest University of Economic Studies, Bucharest, Romania, catalina.toader@fin.ase.ro.
* Corresponding author.

become increasingly sophisticated, making it more challenging for banks to protect their systems and customer data.

2. Problem Statement

An area of research that has received considerable attention is the identification of cyber risks in the banking sector. Researchers have identified various forms of cyber threats that banks face, such as those mentioned above. Moreover, the frequency and severity of cyber threats have been increasing, leading to greater concerns about the ability of banks to protect their systems and customer data. For example, Adrian and Ferreira (2023) found that the number of cyber-attacks on banks has increased significantly in recent years, highlighting the need for banks to be more vigilant and proactive in managing cyber risks.

Another area of research that has received considerable attention is the impact of cyber risks on the banking sector. Cyber risks can have a significant impact on the financial performance and reputation of banks. For example, Nadeau (2021) found that data breaches can lead to a decline in the financial performance of banks, while Bouveret (2018) found that cyber-attacks can result in reputational damage and a loss of customer trust. These findings suggest that cyber risks can have significant consequences for banks, which makes it important for them to have a comprehensive risk management framework in place to manage these risks effectively.

In response to these risks, researchers have studied the best practices for managing cyber risks in the banking sector. These best practices include the development of a robust cybersecurity framework that includes regular risk assessments, employee training, incident response planning, and the implementation of the latest security technologies. For example, Etoom (2023) found that a proactive approach to cybersecurity, including regular risk assessments and employee training, can significantly reduce the impact of cyber risks on banks. Moreover, researchers have emphasised the importance of collaboration between banks, regulators, and other stakeholders to combat cyber threats effectively. For example, Fell et al. (2022) found that regulatory frameworks play a critical role in promoting cybersecurity practices in the banking sector.

Overall, the literature review highlights the importance of digitalisation and cyber risks in the banking sector and the need for banks to adopt a proactive approach to managing these risks. Cyber threats are a growing concern for banks, and their impact can be significant, leading to financial losses, reputational damage, and loss of customer trust. Therefore, banks must have a comprehensive risk management framework in place that includes regular risk assessments, employee training, and the latest security technologies. In addition, collaboration between banks, regulators, and other stakeholders is essential to effectively combat cyber threats.

The literature review also highlights the role of regulatory frameworks in managing cyber risks in the banking sector. Researchers have emphasised the need for regulators to develop clear guidelines and standards for banks to follow in managing cyber risks. These guidelines should be based on best practices and should

be regularly updated to keep up with the evolving threat landscape. Moreover, regulators should conduct regular assessments of banks' cybersecurity frameworks to ensure that they meet these standards.

For example, Crisanto and Prenio (2017) found that regulatory frameworks play a critical role in promoting cybersecurity practices in the banking sector. They argue that regulators should take a proactive approach to cybersecurity, including the development of clear guidelines, regular assessments, and the promotion of information sharing between banks. Similarly, Wilson et al. (2019) found that regulatory frameworks can incentivise banks to invest in cybersecurity by imposing penalties for non-compliance with cybersecurity standards.

In addition to regulatory frameworks, researchers have also emphasised the importance of information sharing between banks and other stakeholders in managing cyber risks. Information sharing can help banks identify potential threats and vulnerabilities more quickly and can facilitate a more coordinated response to cyber incidents. For example, Chamberlain (2018) found that information sharing between banks can help reduce the impact of cyber threats on the banking sector.

The literature review also highlights the role of emerging technologies in managing cyber risks in the banking sector. Researchers have identified various technologies that can help banks improve their cybersecurity frameworks, such as artificial intelligence, blockchain, and cloud computing. For example, Thisarani and Fernando (2021) found that artificial intelligence can help banks detect and respond to cyber threats more quickly and accurately.

Overall, the literature review highlights the multifaceted nature of managing cyber risks in the banking sector. It is not just about implementing the latest security technologies, but also about developing a comprehensive risk management framework that includes regulatory frameworks, information sharing, and collaboration between stakeholders. Moreover, the literature highlights the need for banks to keep up with emerging technologies that can help them improve their cybersecurity frameworks.

Finally, the literature review highlights the potential impact of cyber risks on financial stability. Researchers have noted that a large-scale cyber incident in the banking sector could have significant systemic implications, potentially leading to widespread financial disruption and instability (Kopp et al., 2017). Therefore, managing cyber risks in the banking sector is not just important for individual banks, but also for the stability of the financial system as a whole.

Moving forward, it is essential for banks to develop a comprehensive cybersecurity framework that addresses the unique challenges posed by digitalisation and cyber risks. This framework should include a range of measures, such as employee training and awareness programs, cyber insurance, and collaboration with regulators and other stakeholders.

In conclusion, digitalisation has brought about significant changes in the banking sector, presenting new opportunities for growth and innovation, but also new risks and challenges. Cybersecurity has emerged as a critical issue for banks, as they face an ever-evolving threat landscape that requires constant vigilance and adaptation. By

developing a comprehensive cybersecurity framework that incorporates the latest technological advances and regulatory best practices, banks can better manage their cyber risks and ensure the stability of the financial system as a whole.

3. Research Questions / Aims of the Research

The objective of the research is to explore the challenges faced by banks as they increasingly rely on digital technologies to provide services, and to identify ways to manage the risks associated with cyber threats. This research could provide valuable insights for policymakers, regulators, and practitioners in the banking sector, as well as for academic researchers who are interested in this field.

4. Research Methods

We conducted our research using the qualitative research method, and we started from relevant case studies with banks that faced cyber failures in recent years, trying to gain an in-depth understanding of the challenges they had to overcome and the best practices for managing cyber risks. We selected a sample of 4 internationally active banks that have experienced cyber threats, with effective cyber risk management practices implemented, and explored their experiences and perspectives.

5. Findings

5.1 Cyber Risks in Banking

Cyber risks have become a growing concern for the banking sector in recent years. With the increasing digitisation of banking services, the amount of sensitive information stored and transmitted digitally has also increased, making banks a prime target for cybercriminals.

One of the challenges in managing cyber risks in the banking sector is the constantly evolving nature of cyber threats. Cybercriminals are constantly developing new and more sophisticated methods to circumvent security measures, making it challenging for banks to keep up.

Banks may also consider partnering with cybersecurity firms or other technology experts to enhance their cybersecurity capabilities and stay up-to-date with the latest threats and countermeasures.

Cyber risks in banking refer to the potential threats and vulnerabilities faced by financial institutions in the digital age. These risks can range from cyber-attacks on bank infrastructure and networks to data breaches and theft of sensitive customer information. Cyber risks can have severe consequences for banks, including financial losses, reputational damage, and legal liabilities.

A study by Accenture found that the average cost of a cyber-attack for financial institutions is $18.5 million, being the highest of all industries (Accenture, 2019). These costs can include expenses related to recovery, investigation, legal fees, and fines imposed by regulatory authorities.

Moreover, the banking sector is particularly vulnerable to cyber risks due to the large amounts of valuable data and assets they manage. According to Al-Alawi and Al-Bassam (2020), in 2020, 26 % of financial institutions faced online attacks which materialised through losses of money.

To address these risks, banks are increasingly investing in cybersecurity measures, such as firewalls, intrusion detection systems, and encryption technologies. However, the effectiveness of these measures depends on the bank's ability to detect and respond to potential threats in real-time.

Another challenge in managing cyber risks in the banking sector is the rapid pace of technological change. Banks must continually adapt their cybersecurity measures to keep up with evolving threats and the introduction of new technologies. This requires ongoing investments in research and development, as well as partnerships with technology companies and cybersecurity experts.

In conclusion, cyber risks in the banking sector are a growing concern, and banks must remain vigilant in their efforts to manage these risks. Effective cybersecurity measures, comprehensive frameworks, and ongoing investments in technology and training are crucial to mitigating cyber risks and protecting the integrity and stability of the financial system.

5.2 Risk Management Framework for Cyber Risks

Effective risk management is crucial to managing cyber risks in the banking sector. A robust risk management framework can help banks identify, assess, and manage cyber risks, thus reducing the likelihood and impact of cyber incidents. The following sections provide an overview of the key components of a risk management framework for cyber risks in the banking sector.

5.3 Risk Identification

The first step in managing cyber risks is to identify and assess the risks. Banks need to understand the potential sources of cyber risks, including internal and external threats. Internal threats can include employee errors, system failures, and data breaches, while external threats can include cyber-attacks by hackers, malware, and social engineering. Banks should also consider the potential impact of cyber risks on their operations, reputation, and financial position.

5.4 Risk Assessment

Once the risks have been identified, banks need to assess the likelihood and potential impact of each risk. This assessment should take into account the bank's overall risk appetite and the potential consequences of a cyber-incident. Banks should also consider the effectiveness of their current cybersecurity measures and identify any gaps or vulnerabilities.

5.5 Risk Mitigation

Based on the risk assessment, banks should develop a risk mitigation plan that outlines the actions needed to reduce the likelihood and impact of cyber incidents. This plan should include a range of measures, such as technical controls, security policies and procedures, staff training and awareness, and incident response plans. Banks should also consider the need for cybersecurity insurance to mitigate the financial impact of cyber incidents.

5.6 Risk Monitoring

Effective risk management requires ongoing monitoring and assessment of cyber risks. Banks should establish a process to monitor cyber risks and the effectiveness of their risk mitigation measures. This process should include regular assessments of the bank's cybersecurity posture, vulnerability scanning and testing, and incident reporting and analysis.

5.7 Risk Reporting

Risk reporting is an important component of a risk management framework for cyber risks. Banks should establish a process for reporting cyber risks to senior management and the board of directors. This process should include regular reports on the bank's cybersecurity posture, incident reports and analysis, and recommendations for improving the bank's cybersecurity measures.

The banking sector faces significant cyber risks, and effective risk management is crucial to managing these risks. A robust risk management framework can help banks identify, assess, and manage cyber risks, thus reducing the likelihood and impact of cyber incidents. The components of a risk management framework for cyber risks in the banking sector include risk identification, risk assessment, risk mitigation, risk monitoring, and risk reporting. Banks that implement an effective risk management framework for cyber risks can better protect their operations, reputation, and financial position.

5.8 Regulatory Landscape

The increasing frequency and severity of cyber-attacks in the banking sector have prompted regulatory authorities to introduce new regulations and guidelines to manage cyber risks. The regulatory landscape for cyber risks in the banking sector is complex and rapidly evolving, with multiple regulatory bodies and guidelines across different jurisdictions.

In the United States, the Federal Financial Institutions Examination Council (FFIEC) provides guidelines for financial institutions to manage cyber risks. The FFIEC's Cybersecurity Assessment Tool (CAT) provides a framework for financial institutions to assess their cybersecurity risks and develop a comprehensive cybersecurity risk management program. Additionally, the New York State Department of Financial Services (NYDFS) introduced the first cybersecurity

regulation in the U.S. financial services industry in 2017, requiring financial institutions to establish and maintain a cybersecurity program.

In the European Union, the General Data Protection Regulation (GDPR) introduced in 2018 provides a framework for data protection and cybersecurity. Moreover, in 2019, the European Banking Authority (EBA) has issued guidelines on cyber risk management, stressing the need for a risk-based approach and regular testing and evaluation of cyber risk management processes,

In Asia, the Monetary Authority of Singapore (MAS) introduced the Technology Risk Management Guidelines in 2013, which provide a framework for financial institutions to manage technology risks, including cyber risks. The guidelines require financial institutions to establish a robust governance framework for technology risk management and to conduct regular risk assessments.

Overall, regulatory authorities have recognised the importance of managing cyber risks in the banking sector and have introduced guidelines and regulations to promote cybersecurity risk management. Financial institutions need to comply with these regulations and guidelines and implement robust cybersecurity risk management programs to mitigate the risks of cyber-attacks. Moreover, financial institutions need to ensure that their risk management frameworks are flexible and adaptable to address the rapidly evolving cyber threat landscape.

5.9 Case Studies

In recent years, there have been several high-profile cyber incidents in the banking sector, highlighting the need for effective cyber risk management in the industry.

1. JPMorgan Chase Data Breach (2014)

In 2014, JPMorgan Chase suffered a data breach that affected approximately 76 million households and 7 million small businesses. The breach compromised customer names, addresses, phone numbers, and email addresses, as well as internal data such as employee names and email addresses. The attackers were able to exploit vulnerabilities in JPMorgan Chase's network and gain access to sensitive data.

The cause of the breach was attributed to JPMorgan Chase's failure to patch known vulnerabilities in its systems. In response to the incident, the bank hired additional cybersecurity personnel and invested heavily in improving its cybersecurity defences, including implementing multi-factor authentication and increasing its use of encryption.

2. Bangladesh Bank Heist (2016)

In 2016, hackers stole $81 million from the Bangladesh Bank's account at the Federal Reserve Bank of New York. The attackers were able to gain access to the Bangladesh Bank's systems by stealing employee credentials and then using those credentials to initiate fraudulent transactions.

The cause of the breach was attributed to the Bangladesh Bank's lack of cybersecurity controls, including weak password policies and insufficient network segmentation. In response to the incident, the bank implemented new cybersecurity measures, including two-factor authentication and improved network segmentation.

3. Capital One Data Breach (2019)

In 2019, Capital One suffered a data breach that affected approximately 100 million customers and applicants in the United States and Canada. The breach compromised customer names, addresses, phone numbers, email addresses, dates of birth, and Social Security numbers. The attacker was able to exploit a misconfigured firewall in Capital One's cloud environment to gain access to sensitive data. The cause of the breach was attributed to a misconfiguration in Capital One's cloud environment, which allowed the attacker to gain access to sensitive data. In response to the incident, the bank increased its focus on cloud security, including implementing automated monitoring of misconfigurations and improving its access management processes.

4. Equifax (2017)

In 2017, Equifax, one of the largest credit reporting agencies in the United States, experienced a data breach that affected approximately 143 million customers. The attackers were able to gain access to sensitive customer information, including Social Security numbers, birth dates, and addresses. The breach was attributed to several factors, including unpatched software vulnerabilities, weak passwords, and a lack of employee training. In response, Equifax implemented a number of measures, including upgrading its security systems, enhancing its employee training programs, and increasing its cybersecurity budget.

These case studies illustrate the significant impact of cyber incidents in the banking sector and the importance of effective cybersecurity measures. In each case, the cause of the breach was attributed to specific vulnerabilities or failures in cybersecurity controls, highlighting the need for ongoing risk management and continuous improvement of cybersecurity defences. Additionally, the response measures implemented by each bank demonstrate the importance of investing in cybersecurity measures and taking proactive steps to address vulnerabilities and improve defences.

6. Conclusions

Based on the above analysis, there are several clear recommendations that banks should consider when dealing with cyber risks. These recommendations are summarised in the following matrix:

Table 1. Recommendations for the effective management of cyber risks

Recommendation	Description
Conduct a Risk Assessment	Banks should conduct a comprehensive risk assessment to identify and prioritise their cyber risks. This assessment should include a review of the bank's IT infrastructure, systems, and data, as well as an analysis of potential threats and vulnerabilities.
Develop a Cybersecurity Strategy	Based on the risk assessment, banks should develop a comprehensive cybersecurity strategy that includes policies, procedures, and controls to mitigate identified risks. The strategy should also include measures to monitor and respond to cyber incidents.

Recommendation	Description
Implement Security Controls	Banks should implement security controls to protect their IT infrastructure and data. These controls should include measures such as firewalls, intrusion detection systems, and access controls.
Conduct Employee Training	Banks should provide regular training to employees to raise awareness of cyber risks and provide guidance on how to identify and respond to potential threats. Training should include measures such as phishing simulations and scenario-based training.
Consider Cyber Insurance	Banks should consider purchasing cyber insurance to mitigate the financial impact of cyber incidents. Cyber insurance can provide coverage for losses resulting from cyber events and can be an essential component of a comprehensive cybersecurity framework.
Stay Up-to-Date on Regulations	Banks should stay up-to-date on the regulatory landscape related to cybersecurity. This includes monitoring changes in regulations and guidelines, as well as collaborating with regulators to ensure compliance.
Engage in Information Sharing	Banks should engage in information sharing with other banks, government agencies, and industry groups to stay informed about emerging threats and best practices. This information sharing can help banks to proactively identify and mitigate potential risks.

Source: Authors` contribution.

Overall, banks should take a proactive and comprehensive approach to managing cyber risks. By conducting risk assessments, developing cybersecurity strategies, implementing security controls, providing employee training, considering cyber insurance, staying up-to-date on regulations, and engaging in information sharing, banks can effectively mitigate cyber risks and protect their customers' data and financial assets.

The impact of digitalisation and cyber risks on the banking sector is significant, with the potential for financial losses, operational disruption, and reputational damage. However, banks can mitigate these risks by adopting a proactive approach to cybersecurity, including regular risk assessments, employee training, and the implementation of the latest security technologies. It is also critical for banks to work closely with regulators and other stakeholders to stay informed about the latest threats and to share information to combat cybercrime. By taking a proactive approach, banks can better protect themselves and their customers from cyber risks in the digital age.

References

[1] Adrian, T., Ferreira, C. (2023). Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards, retrieved from https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards.

[2] Al-Alawi, A.I., Al-Bassam, S.A. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector, retrieved from https://www.researchgate.net/publication/337086201_The_Significance_of_Cybersecurity_System_in_Helping_Managing_Risk_in_Banking_and_Financial_Sector.

[3] Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, retrieved from https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.

[4] Chamberlain, K. (2018). Cyber Threats: How Banks Can Share Information Effectively, retrieved from https://bankingjournal.aba.com/2018/11/cyber-threats-how-banks-can-share-information-effectively/.

[5] Crisanto, J.C., Prenio, J. (2017). Regulatory approaches to enhance banks' cyber-security frameworks, retrieved from https://www.bis.org/fsi/publ/insights2.htm.

[6] Etoom, A. (2023). Strategising cybersecurity: Why a risk-based approach is key, retrieved from https://www.weforum.org/agenda/2023/04/strategizing-cybersecurity-why-a-risk-based-approach-is-key/.

[7] Fell, J., de Vette, N., Gardó, S., Klaus, B., Wendelborn, J. (2022). Towards a framework for assessing systemic cyber risk, retrieved from https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202211_03~9a8452e67a.en.html.

[8] Kopp, E., Kaffenberger, L., Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability, retrieved from https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104.

[9] Nadeau, J. (2021). Banking and Finance Data Breaches: Costs, Risks and More to Know, retrieved from https://securityintelligence.com/articles/banking-finance-data-breach-costs-risks/.

[10] Thisarani, M., Fernando, S. (2021). Artificial Intelligence for Futuristic Banking, retrieved from https://ieeexplore.ieee.org/abstract/document/9570253/authors#authors.

[11] Wilson, C., Gaidosch, T., Adelmann, F., Morozova, A. (2019). Cybersecurity Risk Supervision, retrieved from https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2019/09/23/Cybersecurity-Risk-Supervision-46238.