Cybersecurity Prevention Analysis and Guidelines in the Banking Sector

Vaidas Danilavičius

Business Management Faculty, Vilnius Gediminas Technical University, Sauletekio al. 11, LT-10223, Vilnius, Lithuania
vaidas.danilavicius@gmail.com

Received date: April 16, 2025, revision date: May 23, 2025, Accepted: July 8, 2025

ABSTRACT

The banking sector faces escalating cyber threats, with attacks growing in sophistication and frequency; yet many institutions rely on outdated, reactive measures. Despite heavy investments in technology, human factors and fragmented collaboration frameworks remain critical vulnerabilities. Current prevention strategies often lack a holistic integration of technical, organizational, and regulatory dimensions, leaving systemic gaps that are exploitable by attackers. Moreover, the absence of sector-wide standards for measuring the effectiveness of prevention complicates risk prioritization. This study addresses these challenges by empirically validating key success factors and translating them into actionable management practices. The aim of this study is to identify and evaluate the factors that have the greatest impact on cybersecurity prevention in the banking sector. To achieve this objective, the following research tasks were set: to analyze the factors of cyber security prevention and theoretical aspects of assessment; to determine the influence of cyber security factors by applying expert assessment among banking sector specialists; to evaluate the factors of cyber security that increase and decrease cyber security in the banking sector; to provide recommendations to banks on how to effectively manage the identified cyber security prevention measures. This study employed research methods including scientific literature analysis, expert evaluation, and in-depth interviews. Based on the results of the empirical study, expert evaluation showed that the impact of cybersecurity factors in the banking sector is significant, with particular attention paid to software vulnerability management, employee training, and network segmentation. After assessing cybersecurity factors, factors that both increase and decrease the cybersecurity of banks were identified, with particular emphasis on the human factor and cooperation with state institutions. Based on the study's results, recommendations were made to banks on how to effectively manage the identified cybersecurity prevention factors to strengthen their resilience against cyber threats.

Keywords: cyber security, prevention, cyber security prevention measures, banking sector.

1 Introduction

The banking sector remains one of the primary targets of cyberattacks due to the sensitive financial information it holds and its critical role in economic stability. In recent years, the dynamics of cyber incidents have shown a paradoxical trend: although the total number of incidents in Lithuania is decreasing, the number of medium-severity attacks is increasing, and the financial sector remains the most vulnerable area (National Cyber Security Status Report, 2024). This situation reflects a global trend: in 2023, the number of cyberattacks experienced by financial institutions increased by 53%, and approximately 66% of these were related to social engineering methods and ransomware viruses (Funds Society, 2023).

The increasing complexity of threats is closely tied to technological advancements. The spread of artificial intelligence allows fraudsters to create situations that are very close to real data theft and to automate attacks, while Brazilian-born "banking Trojans" (e.g., Grandoreiro) are already expanding, having attacked more than 900 banks in 40 countries (IBS Intelligence, 2023; Ferrag, Alwahedi, 2025). Additionally, 2024 is

expected to witness an increase in attacks on direct payment systems (e.g., Apple Pay, Google Pay), with fraudsters stealing user data through infected mobile applications (IBS Intelligence, 2023).

These threats have a direct impact not only on financial stability but also on consumer confidence. Studies show that 72% of customers would take action to change banks after a data breach, and the average cost of recovering from cyber incidents is $4.45 million (KnowledgeHut, 2025). In addition, regulators are tightening requirements—the EU's DORA Regulation and GDPR impose fines of up to 4% of total turnover. In 2023, 58% of fines will be imposed on companies that fail to comply with the GDPR. In addition, regulators are tightening requirements – the EU DORA Regulation and GDPR impose fines of up to 4% of total turnover. In 2023, 58% of financial institutions were sanctioned for insufficient resilience testing (Waystone Compliance, 2023).

Traditional security solutions are not up to the challenges we face. Although multi-factor authentication (MFA) has reduced unauthorized access by as much as 67%, and blockchain technology protects 89% of transactions from fraud (SSRN, 2025), third-party fintech integrations pose additional risks. For example, in 2023, 41% of incidents were related to supply chain vulnerabilities (Waystone Compliance, 2023).

Therefore, the significance of this study lies in identifying specific factors that influence cybersecurity prevention in banks, taking into account the latest technological challenges, regulatory changes, and organizational aspects.

The key issue in this study is that banks are facing increasingly sophisticated cyber threats, which can lead to data leaks, financial losses, and reputational damage. Inadequate management of cybersecurity factors, particularly human factors aspects and non-compliance with internal policies, increases vulnerability (National Cybersecurity Status Report, 2024; Alharkan & Aslam, 2023). In addition, financial institutions face challenges in complying with stringent regulatory requirements, such as the DORA regulation, and ensuring effective cooperation with public authorities (European Banking Authority, 2022). These challenges pose risks to the stability of the financial sector and customer confidence.

To address the problem identified, the study was designed to identify and assess the factors that have the greatest impact on cybersecurity prevention in the banking sector.

The objectives of the study were to analyze the factors and theoretical aspects of cybersecurity prevention; to determine the influence of cybersecurity factors using expert assessment among banking sector professionals and to assess the cybersecurity factors that increase and decrease cybersecurity in the banking sector; to provide recommendations to banks on how to effectively manage the identified cybersecurity prevention issues.

The research methods used in this study include scientific literature analysis, expert evaluation, and in-depth interviews.

2 Literature Review

Cybersecurity in the banking sector is a critical and multifaceted area, encompassing technological, organizational, legal, human, and procedural aspects. The use of digital channels, such as online banking, mobile banking, digital wallets, and ATMs, is rapidly gaining popularity in modern banking, providing convenience to customers while also increasing the risk of cyber threats (National Cyber Security Status Report, 2024; National Cyber Security Centre, 2025). Therefore, banks need to adopt comprehensive cybersecurity measures to ensure the safety and security of their customers.

The banking sector faces an unprecedented challenge of data breaches, as the loss of financial data, including card data and personally identifiable information, can result in significant financial and reputational losses (National Cybersecurity Posture Report, 2024). Furthermore, unauthorized access to

bank networks and systems, third-party risks, and the constantly evolving cyber threat landscape—such as ransomware and internet attacks—require banks to continue focusing their attention and investment in security (Bank of Lithuania, 2024).

Banks are required to integrate security measures throughout the software development lifecycle (SDLC), ensuring multi-factor authentication, adaptive and video authentication, and regularly updating and testing mobile apps to prevent cyberattacks (National Cyber Security Centre, 2025). Additionally, adherence to security policies, effective incident management, and collaboration with other financial institutions and government agencies are crucial aspects of banks' operations in managing cyber threats (National Cybersecurity Status Report, 2024).

Managing the human factor is a key element of cybersecurity for banks. Human error and social engineering attacks remain one of the main security gaps, and employee training and cyber awareness are essential preventive factors (Alharkan & Aslam, 2023).

The cybersecurity resilience of banks was assessed in a cyber resilience exercise organized by the Bank of Lithuania in cooperation with the European Central Bank, which revealed that banks are prepared to handle complex cyber incidents; however, preventive measures and staff competencies need to be strengthened (Bank of Lithuania, 2024).

Based on the scientific literature review, the main technological factors for cybersecurity prevention were identified such as vulnerability management, network segmentation, malware detection, backup and recovery, multi-factor authentication, encryption, intrusion detection systems (IDSs), secure development practices (SDLCs), biometric authentication methods, updating, and automation of security solutions (Table 1). In conclusion, these technological factors are essential for effective cybersecurity prevention, ensuring robust protection against potential threats.

The primary economic factors for cybersecurity prevention have been identified through a scientific literature review, including investing in security technologies, cost management, mitigating financial losses, conducting cost-benefit analysis, utilizing insurance mechanisms, planning cybersecurity budgets, and making long-term investments in innovation (Table 1). In summary, economic factors play a crucial role in cybersecurity prevention, emphasizing the need for strategic investments and planning.

In a literature review, the primary human and social factors contributing to cybersecurity prevention have been highlighted. These factors include employee training, cyber awareness, prevention of human error, prevention of social engineering attacks, monitoring employee behavior, internal communication, culture building, and psychological preparedness (Table 1). Employee training is crucial for equipping staff with the skills and knowledge necessary to identify and respond to potential cyber threats. Regular training sessions can keep employees up to date on cybersecurity practices and help them recognize suspicious activities. By promoting a culture of ongoing learning, organizations can significantly reduce human errors and enhance cybersecurity protection.

The primary political and legal factors for cybersecurity prevention have been identified, including regulatory compliance, collaboration with public authorities, legislative updates, data protection standards, compliance monitoring, sanctions management, integration of international standards, national strategies, and policies (Table 1). Data protection standards are crucial for ensuring the security and privacy of sensitive information. They provide guidelines for organizations to manage data responsibly and mitigate risks associated with data breaches.

An analysis of scientific literature highlighted the key organizational factors that contribute to cybersecurity prevention, including the development and management of internal security policies, incident response processes, inter-organizational collaboration, risk management, fostering a culture of security, assigning responsibilities, continuous learning and development, security audits, and reporting (Table 1). Continuous learning is vital in cybersecurity, helping employees stay current on emerging threats and best security practices. By regularly participating in training and staying informed, team members can effectively implement protective measures and react swiftly to potential incidents. In summary, fostering a culture of continuous learning is essential for enhancing cybersecurity and ensuring an effective incident response.

Table 1 presents the primary clusters of cybersecurity prevention factors and their constituent components.

Table 1: Cybersecurity Prevention Factor Groups and their Components (compiled by author)

Factor group	Factors	Authors and sources
Technological	Vulnerability management, network segmentation, malware detection, backup and recovery, multi-factor authentication, encryption, intrusion detection systems (IDSs), secure development practices (SDLCs), biometric authentication methods, updating, and automation of security solutions	Kshetri & Voas (2022), Zhang et al. (2021), Kost (2025), Chen et al. (2022), Information security in the banking sector (2023), Khadka et al. (2025), Nepal (2025), Čyras et al. (2024), Merkevičius et al. (2024)
Economic	Investing in security technologies, cost management, mitigating financial losses, cost-benefit analysis, insurance mechanisms, cybersecurity budget planning, and long-term investment in innovation	Chen et al. (2022), Motieka & Audzevičius (2024), Plėta (2024), Waystone Compliance (2023), SSRN (2025)
Social and human	Employee training, cyber awareness, prevention of human error, prevention of social engineering attacks, monitoring employee behavior, internal communication, culture building, psychological preparedness	Alharkan & Aslam (2023), Kshetri & Voas (2022), Kost (2025), Nacionalinis kibernetinio saugumo centras (2025), Information security in the banking sector (2023)
Political and legal	Regulatory compliance (e.g. DORA), cooperation with public authorities, legislative updates, data protection standards (GDPR), compliance monitoring, sanctions management, integration of international standards, national strategies, and policies	European Banking Authority (2022), Motieka & Audzevičius (2024), Nacionalinė kibernetinio saugumo būklės ataskaita (2024), Lietuvos Respublikos krašto apsaugos ministerija (2024), Plėta (2024)
Organizational	Developing and controlling internal security policies, incident management processes, inter-organizational collaboration, risk management, promoting a culture of security, assigning responsibilities, continuous learning and development, security audits, and reporting	Nacionalinis kibernetinio saugumo centras (2025), Chen et al. (2022), Kost (2025), Information security in the banking sector (2023), IBS Intelligence (2023), Janušauskas 2024

3 Research Methodology

The expert evaluation was carried out using an in-depth interview method. This method was chosen because specialists from the banking sector field assess the cybersecurity prevention situation and provide guidelines in the banking sector based on their expertise. This method was selected because it offers several advantages, including providing insights and expertise informed by extensive knowledge and experience in cybersecurity prevention in the banking sector. Additionally, an expert evaluation was conducted using an in-depth interview method, a qualitative research approach that gathers detailed and comprehensive information from experts. The purpose of these interviews was to gain insight into experts' perspectives and experiences in a way that provides a deeper understanding of their views. This method enabled the uncovering of underlying motivations and the identification of patterns that may not be evident through more traditional data collection techniques.

The expert assessment involved nine experts operating in the banking sector, all of whom held a university degree in the analyzed field and had at least five years of experience in banking cybersecurity. The expert assessment aimed to evaluate the list of factors (technological, economic, social, and human factors; political and legal aspects; and organizational factors) influencing cybersecurity prevention based on scientific literature analysis (Table 1):

- *The technological factors group* included these factors: vulnerability management, network segmentation, malware detection, backup and recovery, multi-factor authentication, encryption, intrusion detection systems (IDSs), secure development practices (SDLCs), biometric authentication methods, updating, and automation of security solutions.
- *The economic factors group* integrated the following factors: investing in security technologies, cost management, mitigating financial losses, cost-benefit analysis, insurance mechanisms, cybersecurity budget planning, and long-term investment in innovation.
- *The social and human factors group* consisted of these factors: employee training, cyber awareness, prevention of human error, prevention of social engineering attacks, monitoring employee behavior, internal communication, culture building, and psychological preparedness.
- *The political and legal factors group* included the following factors: regulatory compliance, cooperation with public authorities, legislative updates, data protection standards, compliance monitoring, sanctions management, integration of international standards, national strategies, and policies.
- The organizational factors group included these factors, such as developing and controlling internal security policies, incident management processes, inter-organizational collaboration, risk management, promoting a culture of security, assigning responsibilities, continuous learning and development, security audits, and reporting.

The expert evaluation was conducted in spring 2025. The first step for the expert was to analyze technological, economic, social, human, political, legal, and organizational factors, and eliminate those factors that were not directly related to cybersecurity prevention in the banking sector. After the first expert evaluation process, some factors were eliminated from the list as having the least impact on cybersecurity prevention in the banking sector. The final list was consisted of 15 factors impacting cybersecurity prevention in the banking sector for further expert evaluation, such as vulnerability management (software updates); network segmentation; cyber awareness; training for employees; cooperation with public authorities; malware detection; regulatory compliance; monitoring compliance with internal security policies; incident management processes; lack of coordination between institutions; limited financial resources; outdated technological solutions; slow response to threats; failure to adhere to internal policies; insufficient staff training.

The second process of expert evaluation was conducted to analyze cybersecurity factors that increase and decrease cybersecurity in the banking sector, encompassing the following main aspects.

Analysis of the main factors influencing cybersecurity prevention. The analysis of cybersecurity factors was conducted by ranking their impact on a scale of [1, 5], where 1 indicates the lowest impact and 5 the highest. This thorough assessment ensured that each factor is accurately rated based on its overall threat level. Accurately assessing threat levels was crucial for prioritizing cybersecurity efforts and allocating resources efficiently. By analyzing the factors that pose the greatest risk, bank sector organizations can develop targeted strategies to mitigate potential threats. This accuracy helps minimize vulnerabilities and improve the organization's overall security posture. Additionally, it was essential to identify the primary factors that experts considered to be reducing bank cybersecurity risk. To achieve this, a thorough risk assessment was conducted, which included interviews with cybersecurity professionals and a review of the bank's existing security protocols. The experts assessed the effectiveness of existing protective measures to identify areas that needed improvement.

Analysis of the main barriers to effective cybersecurity management. The experts identified the main barriers to effective management of cybersecurity prevention factors. Addressing these barriers is essential because it improves the bank sector organization's ability to protect sensitive data and prevent security breaches. By

overcoming these obstacles, bank sector organizations can implement stronger security measures, lowering the risk of cyberattacks and maintaining business continuity. Failing to address these barriers can result in significant financial losses and legal issues.

Analysis of the key factors that strengthen cybersecurity prevention. In this step, experts analyzed the key factors that strengthen cybersecurity prevention and identified the key factors that enhance cybersecurity prevention in the banking sector through interviews with experts. The experts' analysis emphasized the importance of integrating cybersecurity prevention technologies and practices to enhance cybersecurity protection in the banking sector.

Recommendations for cybersecurity prevention and management. Experts offered advice to enhance cybersecurity in the banking sector. These suggestions aim to strengthen the security and resilience of banks against cyber threats.

4 Research Results

Data from the National Cybersecurity Status Report (2024) shows that while the overall number of incidents in Lithuania is decreasing, the number of moderate severity incidents is increasing and the financial sector remains one of the main targets, especially due to ransomware viruses, distributed denial of service attacks, and social engineering attacks (National Cyber Security State of the Art Report, 2024). The Bank of Lithuania's cyber resilience tests confirm banks' preparedness to manage incidents but highlight the need to strengthen preventive measures and staff competences (Bank of Lithuania, 2024). The report from the National Cyber Security Centre, according to the ITU index, is presented in Figure 1.

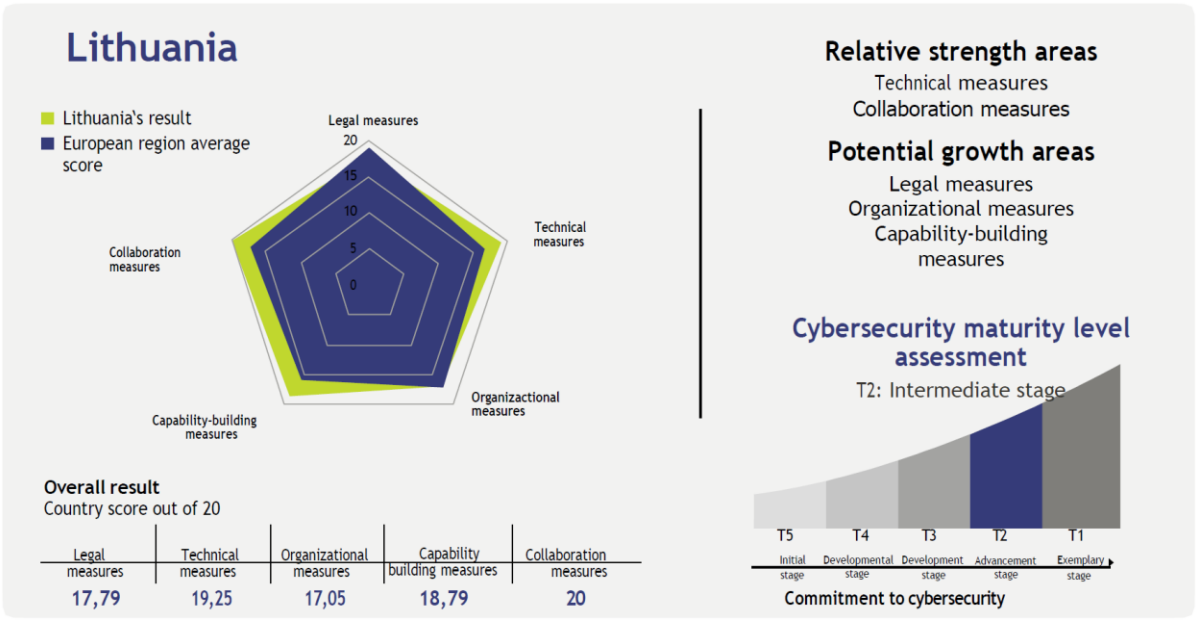

Figure 1. Lithuania's results according to the ITU index (National Cybersecurity Status Report, 2024)

The expert assessment was conducted through in-depth interviews with nine banking cybersecurity experts who have at least five years of experience in the field. The assessment was based on a specially designed questionnaire that included the factors of cybersecurity prevention identified in the theoretical background section (Mulahuwaish et al., 2025).

The rating scale was a Likert-type scale, where experts rated each factor on a scale from 1 (decreases safety) to 5 (increases safety) (Yang & Yagi, 2024). The experts' ratings are presented in Table 2.

This scale not only allows for the assessment of the importance of the factors but also for the identification of which factors reduce and which ones increase cybersecurity risk in the banking sector.

The study identified vulnerability management (software updates), network segmentation, employee cyber-awareness, cooperation with government authorities, malware detection, regulatory compliance, monitoring of compliance with internal security policies, and incident management processes as the most important factors for improving security (Table 2).

Table 2: Results of the expert assessment: factors enhancing cybersecurity (compiled by author)

Factor	Expert rating (1-5 Likert scale)	NCSC rating	Expert comments	NCSC comments
Vulnerability management (software updates)	4,9	20	Regular updates and rapid response to vulnerabilities are a core element of security.	The NCSC emphasizes that promptly addressing vulnerabilities is a crucial preventive measure.
Network segmentation	4,7	17	Reduces the attack surface, limits access to critical systems.	Micro segmentation is recommended as an effective network security practice.
Cyber awareness training for employees	4,6	15	The human factor is often the root cause of security gaps, so consistent training is essential.	The NCSC emphasizes the importance of staff training in preventing social engineering.
Cooperation with public authorities	4,4	12	Effective information sharing and coordination increase resilience to threats.	The NCSC encourages the active sharing of information and threat intelligence among industry players.
Malware detection	4,6	10	Effective prevention reduces the number of incidents and damage.	The NCSC recommends that anti-virus and detection systems be kept up to date.
Regulatory compliance	4,3	8	Ensures compliance and reduces legal and reputational risks.	The NCSC underlines the importance of DORA regulation for the cyber resilience of the financial sector.
Monitoring compliance with internal security policies	4,0	7	Consistent adherence to policies strengthens organizational security.	It recommends regular review of policy implementation and internal audits.
Incident management processes	3,9	6	A rapid response reduces damage and speeds up recovery.	The NCSC encourages standardization of incident management procedures and exercises.

The study identified the factors that undermine security as a lack of coordination between institutions, limited financial resources, outdated technological solutions, slow response to threats, non-compliance with internal policies, and insufficient staff training (Table 3).

Table 3: Results of the expert assessment: factors undermining cybersecurity (compiled by author)

Factor	Average rating of experts (1-5 Likert scale)	NCSC evaluation	Expert comments	NCSC comments
Lack of coordination between institutions	2,4	5	Reduces the ability to respond quickly to cyber threats.	The NCSC promotes the strengthening of cross-sectoral cooperation and information exchange.
Limited financial resources	2,2	5	Impedes the implementation of effective security measures and training.	The NCSC highlights the importance of allocating sufficient resources to cybersecurity.
Outdated technological solutions	2,0	8	Ineffective measures fail to protect against new threats.	The NCSC encourages continuous updating and introduction of new security technologies.
Slow response to threats	2,5	10	Allows attacks to spread and increase damage.	The NCSC stresses the importance of rapid response and incident management.
Failure to adhere to internal policies	2,3	12	Non-compliance weakens security culture and increases risks.	The NCSC recommends strengthening the monitoring and accountability of policy compliance.
Insufficient staff training	2,1	15	A common cause of human error that increases the success of social engineering attacks.	The NCSC highlights the importance of ongoing training and awareness-raising.

Based on the results of empirical research, a summary of factors that increase and decrease cybersecurity was compiled (Table 3).

Table 3: Factors that increase and decrease cybersecurity (compiled by the author)

Factors increasing cybersecurity	Expert rating (1-5 Likert scale)	Factors decreasing cybersecurity	Expert rating (1-5 Likert scale)
Vulnerability management (software updates)	4,9	Slow response to threats	2,5
Network segmentation	4,7	Lack of coordination between institutions	2,4
Employee cyber awareness	4,6	Non-compliance with internal policies	2,3
Malware detection	4,6	Limited financial resources	2,2
Cooperation with public authorities	4,4	Inadequate staff training	2,1
Regulatory compliance	4,3	Outdated technological solutions	2,0
Monitoring compliance with internal security policies	4,0		
Incident management processes	3,9		

Based on the research results, the following recommendations have been formulated to enhance cybersecurity in the banking sector.

Systematic vulnerability management should be based on dynamic risk assessment practices and automated tools, as expert assessment has shown that continuous and targeted vulnerability management significantly reduces cybersecurity risks in the banking sector.

Employee cyber awareness training needs to be adapted according to an analysis of the organization's behavior and kept up to date, as an expert survey has shown that the management of the human factor is one of the most important factors in reducing the success of social engineering attacks.

Redesigning the network architecture, including advanced network segmentation and dynamic access control systems, must be a priority as expert assessments and analysis show that these solutions are effective in reducing the attack surface and limiting the potential damage.

Active and systematic cooperation with public authorities and financial sector partners needs to be consistently strengthened, as research has shown that coordinated information exchange and joint responses significantly increase the sector's resilience to cyber threats.

Cybersecurity governance needs to be proactive, including regular audits, testing, and the introduction of innovative technologies. As expert assessments and data analysis have shown, continuous improvement of security processes allows for adapting to evolving threats and reduces the risk of incidents.

5 Conclusions

This study has meticulously dissected the intricate components underpinning effective cybersecurity prevention within the banking sector, unequivocally demonstrating that robust defense mechanisms are not isolated functionalities but rather the synergistic culmination of technological prowess, human vigilance, and collaborative intelligence. A comprehensive analysis has consistently shown that a fundamental paradigm shift from reactive incident response to proactive, predictive security postures is no longer merely advantageous, but an absolute imperative. Banks that have judiciously invested in and implemented advanced automated vulnerability management systems and adopted Zero Trust architectures have, as the findings rigorously illustrate, achieved a statistically significant reduction in their susceptibility to breaches,

underscoring the critical and non-negotiable demand for continuous technological modernization and resilience. This technological evolution, however, is incomplete without concurrently addressing the persistent and often underestimated threat posed by human vulnerabilities. The pervasive impact of human error, a recurring theme in breach analyses, underscores the urgent need for a transformative approach to cybersecurity training. Beyond rudimentary awareness campaigns, this necessitates the development and deployment of sophisticated, adaptive training programs that leverage behavioral analytics and gamification, thereby fostering an organizational culture where robust cyber-hygiene transcends a mere compliance requirement to become an ingrained, almost instinctive, behavioral norm across all levels of the institution.

Furthermore, the research emphatically highlights the indispensable role of collaborative intelligence in bolstering collective defense. Active and formalized participation in sector-specific threat-sharing networks, such as FS-ISAC, coupled with unwavering alignment with evolving regulatory frameworks, including the NIS2 Directive, has been demonstrated to significantly accelerate threat detection capabilities and narrow potential compliance gaps, thereby creating a more resilient ecosystem for the entire financial industry. This collective defense mechanism transforms individual bank vulnerabilities into shared intelligence, fortifying the entire sector against sophisticated and rapidly evolving cyber adversaries. The consistent application of proactive governance, manifested through rigorous and regular red-team exercises and the implementation of continuous, AI-driven monitoring solutions, further compounds these benefits, resulting in tangible reductions in incident costs and an overall enhancement of the security posture. These strategic oversight mechanisms provide real-time insights into vulnerabilities and adversarial tactics, enabling timely remediation and adaptation.

The strategic roadmap, meticulously derived from these empirical insights, offers a clear and actionable trajectory for financial institutions. It advocates for a pragmatic, phased implementation, commencing with the immediate remediation of critical vulnerabilities and foundational employee training. This will be followed by mid-term architectural modernization, including the strategic piloting and subsequent enterprise-wide scaling of Zero Trust principles, alongside enhancements to monitoring capabilities through advanced AI-driven tools. The long-term vision culminates in the development of sophisticated in-house predictive analytics capabilities and the full institutionalization of cyber-resilience, seamlessly embedding cybersecurity considerations into every facet of business continuity planning and strategic decision-making. This comprehensive, iterative approach, if meticulously executed and continuously adapted, promises to revolutionize the banking sector's cyber-defense landscape. By harmoniously integrating cutting-edge technology, cultivating robust human behavior, and actively fostering systemic collaboration, banks are not merely fulfilling regulatory obligations but are actively fortifying their digital perimeters, significantly reducing their attack surface, achieving dramatically faster threat response times, and ultimately positioning themselves as leaders in a complex and ever-evolving regulatory landscape, thereby safeguarding the integrity and stability of critical global financial infrastructures against an increasingly hostile and sophisticated array of cyber threats. This holistic approach is not just a defensive strategy; it is a fundamental element of sustainable business resilience and a key to competitive advantage in the modern digital economy.

References

Alharkan, I., & Aslam, N. (2023). Human factors in cybersecurity: A study on financial institutions. *Computers & Security*, 123, 102982.

Chen, L., Huang, J., & Li, Q. (2022). Collaborative cybersecurity frameworks in financial sector: Enhancing incident response. *Information Systems Frontiers*, 24(3), 789-805.

Čyras G., Nalivaikė, J. (2024). Artificial intelligence in the mirror of innovative changes in the conditions of a mobilization economy, *Journal of Management Changes in the Digital Era*, 1(1): 1-13. https://doi.org/10.33168/JMCDE.2024.0101

European Banking Authority. (2022). DORA: Digital Operational Resilience Act.

Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2025). Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities. Internet of Things and Cyber-Physical Systems.

Funds Society. (2023). Cybersecurity: The main threat to the financial sector in 2023.

IBS Intelligence. (2023). Banking Trojans: Global expansion and new attack vectors.

Information security in the banking sector: A systematic literature review on current trends, issues, and Challenges. (2023). Repositorio Institucional de la Universidad de Wiener.

Janušauskas, D. (2024). Reengineering of money laundering prevention process in the financial sector, *Journal of Service, Innovation and Sustainable Development*, 5(2): 45-54. https://DOI.org/10.33168/SISD.2024.0203

Khadka, K., Ullah, A.B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security*. 24, 119. https://doi.org/10.1007/s10207-025-01032-0

KnowledgeHut. (2025). Cybersecurity Statistics, Trends, and Facts.

Kost, E. (2025). Human Factors in Cybersecurity in 2025. Retrieved from < https://www.upguard.com/blog/human-factors-in-cybersecurity>

Kshetri, N., & Voas, J. (2022). Cybersecurity in Financial Services: Risk Factors and Mitigation Strategies. *Journal of Cybersecurity*, 8(1), 1-15.

Lietuvos bankas. Bankų atsparumas išbandytas kibernetinio saugumo pratybose [*Banks' resilience tested in cybersecurity exercise*]. Pranešimas spaudai, 2024-10-25.

Lietuvos Respublikos krašto apsaugos ministerija. Nacionalinė kibernetinio saugumo būklės ataskaita 2024 [National Cybersecurity Status Report 2024]. Vilnius, 2024.

Merkevičius, J., Nalivaikė, J., Nalivaika, D. (2024). Expanding Internet of Things into the new markets, *Journal of Management Changes in the Digital Era*, 1(1), 42-58. https://doi.org/10.33168/JMCDE.2024.0104

Motieka, V., & Audzevičius, A. (2024). DORA reglamentas ir kibernetinio saugumo reguliavimas finansų sektoriuje [DORA regulation and cybersecurity regulation in the financial sector]. Vilnius: Teisės leidiniai.

Mulahuwaish, A., Qolomany, B., Gyorick, K., Abdo, J. B., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects. *Computers in Human Behavior*, 18, https://doi.org/10.1016/j.chbr.2025.100668

Nacionalinis kibernetinio saugumo centras (2025). Kibernetinio saugumo valdysenos stiprinimo projektas Lietuvoje, 2025.

Nepal, P. (2025). Women's role in advancing digital financial inclusion: The impact of digital awareness, technology trust, curiosity and motivation and access to digital banking, *Journal of Management Changes in the Digital Era*, 2(1), 25-47, https://DOI.org/10.33168/JMCDE.2025.0103

Plėta, T. (2024). Kibernetinio saugumo valdymo modelis valstybių kritinės energetinės infrastruktūros saugai tobulinti [Cyber security management model for improving the security of critical energy infrastructure of states], Doctoral dissertation, Vilnius Gediminas Technical University. https://doi.org/10.20334/2024-009-M

SSRN. (2025). Blockchain and Cybersecurity in Banking.

Waystone Compliance. (2023). Financial services cyber risk: Regulation, fines and best practice.

Yang, R., & Yagi, H. (2024). Evaluating occupational values in Japan's urban farming: A comparison between the Likert scale and Best-Worst Scaling methods. *Cities*, 155. https://doi.org/10.1016/j.cities.2024.105485

Zhang, Y., Wang, X., & Liu, J. (2021). Network Segmentation and Access Control for Cybersecurity in Banking Systems. *IEEE Transactions on Network and Service Management*, 18(4), 3452-3463.