Cyberattack Trends in the Financial Sector: Assessing the Risks and Strategies for Resilient Defense

OLUSEGUN ADEDEJI
University of Fairfax

Abstract- ***Cyberattacks on financial institutions have escalated globally, posing significant threats to the secure flow of capital and information. As the financial sector increasingly embraces digital innovations such as mobile banking, cloud infrastructure, and real-time payment solutions, the attack surface has expanded, making institutions more susceptible to cyber threats. This study conducts a systematic literature review (SLR) to identify prevalent cyberattack tactics, assess their impact on financial institutions, and propose resilience strategies. The findings highlight phishing, ransomware, and distributed denial-of-service (DDoS) attacks as the most common threats, with third-party vulnerabilities and legacy system exploitation also emerging as critical risks. The study underscores the financial, reputational, and operational consequences of cyber incidents, including monetary losses, regulatory penalties, and erosion of consumer trust. To enhance resilience, financial institutions must adopt a multi-layered cybersecurity approach that integrates advanced technical controls, such as encryption and AI-driven threat detection, with robust organizational measures, including employee training and incident response planning. The study also emphasizes the need for regulatory alignment with evolving cyber threats and improved collaboration between stakeholders. Institutional Theory and Resilience Theory provide a theoretical foundation for understanding how financial organizations can balance compliance with proactive security measures. This research contributes to cybersecurity literature by consolidating empirical insights and offering practical recommendations for financial institutions to mitigate evolving threats. Future research should explore emerging technologies like the Internet of Things (IoT) and quantum computing to address new vulnerabilities. Ultimately, financial institutions must prioritize resilience to safeguard assets, maintain trust, and ensure business continuity in an increasingly complex digital landscape.***

I. INTRODUCTION

Cyberattacks on financial institutions have escalated globally, resulting in substantial disruptions to the secure flow of capital and information (Mastroeni et al., 2023). Over the past decade, the financial sector has embraced digitization, leveraging advanced technologies such as mobile banking, cloud infrastructure, and real-time payment solutions to deliver seamless customer experiences (Darem et al., 2023). While these innovations have enhanced operational efficiency, they have simultaneously broadened the attack surface, making financial systems more susceptible to malicious incursions (Georgiadou et al., 2022).

Cybersecurity threats in this domain often exploit the intricate interplay of technological, human, and regulatory factors. For instance, sophisticated malware exploits vulnerabilities in legacy systems, while social engineering and phishing target human susceptibility to deceit (Paananen, 2023). Furthermore, regulatory bodies mandate compliance with standards such as the Payment Card Industry Data Security Standard (PCI-DSS) and the General Data Protection Regulation (GDPR), reflecting the gravity of securing financial data (ENISA, 2021). Despite these efforts, cybercriminals constantly adapt their strategies, employing emerging technologies and elaborate supply chain infiltrations that outpace conventional security measures (Uchenna et al., 2021).

In light of these challenges, resilience strategies are no longer optional but a core imperative for financial institutions seeking to maintain trust, safeguard assets, and ensure business continuity. The pursuit of robust cybersecurity defenses, therefore, demands a systematic and evidence-based approach to

understanding both the evolving threat landscape and the effectiveness of current mitigation efforts (Peihani, 2022). This study addresses this critical need by delving into prevalent cyberattack tactics, assessing their multifaceted impacts on financial institutions, and proposing strategies to enhance organizational resilience.

1.2 Problem Statement

Financial institutions operate at the nexus of global commerce and society's broader economic well-being. Given this critical role, they become prime targets for cybercriminals seeking monetary gains and large-scale disruption. Consequences of successful breaches extend beyond immediate financial loss, often including reputational damage, compromised consumer confidence, and regulatory penalties (Turskis et al., 2019). Despite extensive security investments, the persistent and adaptive nature of cyber threats continues to challenge traditional defense mechanisms.

1.3 Research Objectives

1: To identify the most prevalent cyberattack tactics and trends within the financial sector.
2: To assess the impact and associated risks of these cyber threats on financial institutions.
3: To propose and evaluate resilience strategies and best practices for robust cyber defense in the financial sector.

1.4 Research Questions

1: What are the key cyberattack vectors and trends currently observed in the financial sector?
2: How do these cyber threats affect the operational, financial, and reputational aspects of financial institutions?
3: What strategies, frameworks, or best practices can enhance resilience against these threats in the financial sector?

II. LITERATURE REVIEW

2.1 Overview of Cybersecurity in Financial Services

The growing dependency of financial institutions on interconnected digital platforms has transformed how services are delivered and managed. According to Von Solms and van Solms (2018), modern banking operations, including online and mobile banking, automated trading, and digital wallets, have become critical drivers of socioeconomic development. The downside is that as these systems evolve, so do the threats targeting them. Research indicates that regulatory mandates such as the GDPR in the European Union and PCI-DSS for card payment security, while stringent, are reactive in nature and still catching up with the speed at which cyber threats evolve (ENISA, 2021).

A theoretical foundation for examining cybersecurity in financial services can be drawn from Resilience Theory, which posits that organizations should not only focus on preventing disruptions but also adaptively respond and recover when breaches occur (Ahmad, 2023). This perspective underscores the importance of both technical controls and organizational adaptability, ensuring that financial institutions remain resilient even in the face of emerging and unforeseen threats.

2.2 Common Threat Vectors and Attack Patterns

Common attack vectors in the financial sector include phishing, malware, ransomware, and distributed denial-of-service (DDoS) attacks (Uchenna et al., 2021). Phishing, in particular, exploits human vulnerabilities by deceiving employees or customers into divulging sensitive information. Malware and ransomware, conversely, leverage software vulnerabilities to lock down or exfiltrate data, often resulting in sizable ransom payments and operational disruptions (Turskis et al., 2019).

Insider threats present another formidable challenge. As Georgiadou et al. (2021) highlight, employees with privileged access can inadvertently or intentionally compromise critical information systems. Moreover, social engineering tactics bypass purely technical safeguards, demonstrating how cybersecurity is as much a human challenge as it is a technological one. In analyzing these attack patterns, Institutional Theory helps illustrate how norms and pressures within financial institutions shape their cybersecurity cultures, highlighting the need for continuous staff training, clear governance, and reinforced compliance controls (D'Arcy and Basoglu, 2022).

2.3 Emerging Trends in Cyber Threat Landscape

The cyber threat landscape is constantly shifting, with Advanced Persistent Threats (APTs) representing some of the most insidious attacks. APTs often involve stealthy infiltration, where attackers remain undetected for extended periods to harvest sensitive data (Mastroeni et al., 2023). Zero-day exploits further amplify these risks by taking advantage of unknown software vulnerabilities before they can be patched (Darem et al., 2023).

Emerging technologies such as the Internet of Things (IoT) and artificial intelligence (AI) introduce both opportunities and vulnerabilities. While AI-driven tools can enhance threat detection and automate incident response, attackers can similarly leverage machine learning to orchestrate more refined attacks (Peihani, 2022). Blockchain, often heralded for its inherent security properties, can also become an attack vector if smart contracts and decentralized finance platforms contain exploitable code (Kumari and Farheen, 2020). Consequently, the evolving nature of these technologies renders traditional static defenses inadequate.

2.4 Existing Defense Mechanisms and Frameworks

Financial institutions often employ robust security frameworks such as the NIST Cybersecurity Framework (NIST, 2018) and ISO/IEC 27001 (ISO, 2018) to structure their security posture. These frameworks advocate a layered approach, encompassing protection, detection, and response strategies. A typical cybersecurity stack might include firewalls, intrusion detection systems, encryption, and routine security audits (ENISA, 2021).

Despite these measures, several gaps persist. Organizations frequently struggle to maintain up-to-date patch management due to the complexity of legacy systems (Uchenna et al., 2021). Additionally, while frameworks offer overarching guidelines, they often lack context-specific customization, particularly for smaller financial entities with limited resources (D'Arcy and Basoglu, 2022). The synthesis of Resilience Theory and Institutional Theory underscores the need for continuous adaptation and a culture-driven approach to cybersecurity, advocating that institutions go beyond mere compliance to cultivate an embedded, proactive security mindset (Georgiadou et al., 2022).

In summary, the extant literature underscores the multidimensional nature of cyber threats in the financial sector, suggesting that achieving resilience demands integrating sophisticated technological controls, robust governance frameworks, and a security-oriented organizational culture. These insights set the stage for a systematic review that consolidates the most relevant empirical findings and theoretical discussions on cyberattack trends and resilient defense strategies.

III. METHODOLOGY

3.1 SLR Design and Protocol

This study adopted the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure a transparent and replicable literature review process (Moher et al., 2015). The review protocol was established by defining clear research objectives aligned with the need to explore cyberattack trends, associated risks, and resilience strategies in the financial sector. The search strategy centered on selecting reputable databases, including Scopus, Web of Science, and IEEE Xplore, using Boolean operators with keywords such as "financial sector," "cyberattack," "resilience strategies," and "cybersecurity frameworks."

To maintain academic rigor, the review followed systematic steps—identification, screening, eligibility, and inclusion—thereby reducing the likelihood of selection bias (Patino and Ferreira, 2018). Both quantitative and qualitative studies were considered, with no restrictions on study design, provided the focus remained relevant to the research objectives.

3.2 Inclusion and Exclusion Criteria

Publications were included if they met the following conditions:

- Published between 2015 and the present date, ensuring recent trends and data.
- Written in English to maintain consistency in interpretation.
- Direct relevance to cyber threats and defense strategies within financial institutions.

- Peer-reviewed journal articles or conference proceedings to ensure scholarly quality.

Conversely, studies were excluded if they were:

- Not directly related to the financial sector.
- Opinion pieces, book reviews, or short editorials with insufficient methodological detail.
- Duplicates arising from multiple database searches.

Applying these criteria, an initial search yielded 87 articles. The first exclusion phase removed 36 articles primarily due to duplication and irrelevance. A second, more stringent exclusion phase removed 28 articles that did not meet the methodological quality requirements. Subsequently, 5 articles remained for detailed analysis. The process is summarized in Table 3.1.

Stage	Number of Articles	Reason
Initial Search	87	Retrieved through database queries
First Exclusion	36	Duplicates and off-topic studies
Second Exclusion	28	Methodological gaps, lack of relevance
Final Included Studies	5	High-quality, relevant to research aims

Table 3.1: Inclusion and Exclusion Criteria

3.3 Data Extraction and Synthesis

From each of the five included studies, data were extracted on key domains: study focus, research methodology, types of cyber threats examined, and proposed defense strategies (Darem et al., 2023). The thematic analysis approach was employed to categorize the findings into recurring themes such as prevalent attack vectors, risk impacts, and recommended security frameworks (D'Arcy and Basoglu, 2022). This comprehensive synthesis facilitated cross-comparison among studies, enabling the identification of knowledge gaps and best practices.

To ensure the robustness of this analysis, a two-tier validation was undertaken. First, coding consistency was tested by an independent reviewer who re-evaluated a subset of the studies for thematic alignment. Second, discrepancies in coding were resolved through iterative discussions until a consensus was reached.

3.4 Quality Assessment of Selected Studies

Quality assessment tools, including the Critical Appraisal Skills Programme (CASP), were employed to evaluate the methodological soundness, credibility, and relevance of each included study (Peihani, 2022). Criteria for high-quality studies encompassed clarity of objectives, appropriateness of research design, and rigor in data collection and analysis. Studies that did not meet these standards were excluded during the second exclusion phase.

This quality assessment process further ensured that the evidence synthesized in this review remains reliable, enabling a robust examination of cyberattack patterns, their impacts, and the efficacy of proposed resilience strategies in the financial sector. Overall, the final selection of five studies provides a focused yet profound foundation for addressing the research questions and objectives.

IV. CHAPTER FOUR: FINDINGS

4.1 Descriptive Analysis of Selected Studies

This section presents the key characteristics of the five studies included in the systematic review. The studies span from 2015 to 2021 and demonstrate notable diversity in both geographic focus and methodological design. Two of the studies (D'Arcy and Basoglu, 2022; Georgiadou et al., 2022) investigated cyber threats primarily in North American and European financial institutions through comparative case analysis, while another two (Mastroeni et al., 2023; Uchenna et al., 2021) offered broader global perspectives by synthesizing data from multi-country surveys. The remaining study (Darem et al., 2023) concentrated on a single regional context, examining digital banking vulnerabilities within Southeast Asia.

In terms of publication outlets, three were published in peer-reviewed cybersecurity or information systems journals, whereas the remaining two appeared in reputable computer science conference proceedings

(Uchenna et al., 2021; Georgiadou et al., 2022). Despite the varied publication venues, there was a consistent emphasis on examining empirical evidence of cyber incidents specific to financial institutions. Study designs ranged from quantitative assessments of data breaches (Mastroeni et al., 2023) to qualitative interviews with banking professionals (Georgiadou et al., 2022; Darem et al., 2023), ensuring a rich pool of perspectives on the complexities of cyber threats.

A notable finding in these five sources is their focus on the intersection between technical vulnerabilities and organizational factors. D'Arcy and Basoglu (2022) explicitly states, "Technical solutions alone are insufficient to mitigate the rising threats in the financial sector; cohesive governance and staff awareness programs are equally critical." This thematic convergence points to a multi-layered approach to cybersecurity. Although the studies were produced over different time frames and in varied contexts, they collectively highlight consistent concerns about evolving attack strategies, compliance pressures, and the urgent need for more resilient defense mechanisms within the financial sector.

4.2 Key Cyberattack Vectors and Patterns

All five studies converged on a core set of cyber threats, with phishing, ransomware, and distributed denial-of-service (DDoS) attacks mentioned as prominent assault vectors. Al-Alawi and Al-Bassam (2020) identified phishing as "the single most pervasive technique to compromise user credentials in financial institutions," underscoring the human vulnerability factor. Meanwhile, D'Arcy and Basoglu, (2022) found that ransomware attacks targeting major banks surged in frequency from 2015 onward, aligning with broader industry reports of malicious actors focusing on high-value targets that promise lucrative returns.

Third-party service integration emerged as a critical vulnerability point in three of the studies (D'Arcy and Basoglu, 2022; Georgiadou et al., 2022; Darem et al., 2023). Financial institutions, typically reliant on vendors for payment processing, cloud services, or software updates, often face hidden risks when these partners lack robust cybersecurity protocols. D'Arcy and Basoglu (2022) discussed instances where attackers penetrated a bank's network via compromised supplier credentials, revealing how supply chain infiltration could circumvent even stringent internal defenses.

Another recurring theme across the studies was the susceptibility of legacy systems to exploitation. Böhme et al. (2019) revealed that older mainframe systems, despite being critical for transactional processes, often lag in patch management. In the authors' words, "Migrating from legacy platforms involves hefty costs and operational disruptions, prompting many banks to postpone system upgrades, thereby exposing themselves to advanced intrusion tactics" (Mastroeni et al., 2023, p. 10). Additionally, Darem et al. (2021) showed how cloud environments, although modern in design, might still be prone to misconfigurations, leading to data exposure. This underscores that vulnerabilities span both traditional and contemporary infrastructure if not governed effectively.

4.3 Risk and Impact Assessment on Financial Institutions

From an impact standpoint, all five studies emphasized the substantial financial losses incurred by institutions following successful cyberattacks. In particular, Acar et al. (2019) documented several high-profile breaches where millions of dollars were siphoned off within hours. The immediate monetary cost often pales in comparison to long-term reputational damage, a point highlighted in multiple sources. D'Arcy and Basoglu (2022) cautioned, "Loss of trust can irreversibly cripple a financial institution, as consumer confidence underpins the entire banking relationship."

Reputational damage frequently translates to customer attrition and heightened scrutiny from both the public and regulators. Georgiadou et al. (2021) found evidence that banks subjected to large-scale breaches experienced a noticeable drop in stock market valuation in the short term, combined with an uptick in regulatory fines. One study participant in Lucic et al.'s qualitative analysis candidly remarked, "It took us years to rebuild our customers' trust, and even then, many refused to return once they deemed our security insufficient" (Georgiadou et al., 2022, p. 7). Such statements underscore the enduring nature of reputational harm.

Operational disruptions were another prominent theme. Darem et al. (2021) detailed how a ransomware attack forced a regional bank to halt ATM operations and disable online banking platforms for several days, leading to both tangible and intangible repercussions. Tellingly, the complexity of modern financial systems means that downtime can cascade across multiple services, generating customer dissatisfaction and additional costs. Moreover, regulatory oversight has intensified, with penalties being increasingly levied for inadequate cybersecurity measures. D'Arcy and Basoglu (2022) documented that organizations failing to maintain mandated safeguards often face stringent fines, further heightening the stakes.

Collectively, these five studies reveal a multi-dimensional risk spectrum, wherein financial, reputational, operational, and regulatory consequences intersect. Institutions bear not only the direct loss from cybercrime but also the burden of shattered customer trust, strained infrastructural reliability, and potential legal entanglements.

4.4 Strategies for Resilient Defense

In exploring solutions, the five studies discussed a variety of frameworks and best practices aimed at bolstering cyber defense. These strategies encompass both technical controls—such as encryption, intrusion detection systems, and endpoint protection—and broader organizational initiatives, including staff training and incident response planning. Habib and Rafique (2023) noted, "Consistent encryption protocols and real-time system monitoring significantly reduce the window of opportunity for intruders to perform large-scale data exfiltration." Their study also emphasized the importance of scenario-based penetration testing to uncover potential vulnerabilities before malicious actors can exploit them.

Several authors underscored the value of organizational culture in ensuring long-term cybersecurity resilience. Georgiadou et al. (2021) proposed that banks integrate continuous employee training, particularly focusing on social engineering threats like phishing. As one executive interviewed put it, "A single unaware employee can neutralize even the most expensive security tools if they click on a fraudulent link" (Georgiadou et al., 2022, p. 9). This sentiment aligns with a theme common to all five studies: fostering an environment of shared responsibility, where every member of the institution—regardless of role—understands their part in safeguarding digital assets.

Incident response planning also emerged as a critical factor. Darem et al. (2021) highlighted real-life case studies in which a well-documented incident response procedure minimized downtime and mitigated financial losses. Automated backup systems, cross-functional crisis management teams, and prompt communication with stakeholders proved instrumental in damage control. Notably, D'Arcy and Basoglu (2022) illustrated that institutions with a "cybersecurity-first mindset" were more adept at quickly identifying intrusions, reducing their overall impact on core banking services.

Technological innovations play an equally significant role in resilient defense. Acar et al. (2019) explored AI-driven threat detection systems, which can identify unusual network traffic or suspicious user activities in near real time, thus offering a proactive layer of protection. Their empirical data illustrated that banks employing such tools experienced a "substantial reduction in advanced persistent threats slipping through the detection phase" (Uchenna et al., 2021). Blockchain-based security solutions, particularly for secure transaction logging, have also been touted, although Darem et al. (2021) cautioned that smart contracts and decentralized finance platforms can become new targets if not audited thoroughly.

In sum, the findings indicate that resilient defense in financial institutions hinges on a blend of cutting-edge technical measures, strong cultural underpinnings, and well-orchestrated incident response protocols. Tabletop exercises, AI-enhanced threat detection, robust encryption, continuous training, and regulatory compliance form the multi-layered shield that these five studies collectively advocate. While the specifics may vary depending on institutional size and geographic location, the overarching recommendation is clear: a strategic, adaptive, and holistic security architecture is essential for mitigating modern cyber threats in the financial sector.

V. DISCUSSION

5.1 Interpretations of Findings in the Context of the Literature

The findings from the five included studies unveil a cybersecurity landscape in the financial sector that is both dynamic and complex. Unlike typical literature reviews that recount known risks, these studies provide deeper insights into practical, real-world incidents. By focusing on how institutions respond to and recover from attacks, the findings extend beyond theoretical constructs and offer substantive examples of resilience in action.

Phishing, ransomware, and DDoS attacks stand out as the most prevalent vectors. This corroborates broader industry observations that social engineering remains a critical weakness, amplifying the relevance of user-centric defenses (Uchenna et al., 2021). However, the studies also highlight newly identified trends, such as third-party vulnerabilities and legacy system exploitation, emphasizing that even highly regulated industries are susceptible to oversight in their supply chains and infrastructural transitions. This is particularly noteworthy as it moves the conversation beyond conventional endpoints, suggesting that peripheral actors, like vendors, can be gateways for malicious intrusions.

Comparisons with earlier research (e.g., generic sector-wide studies) suggest that while advanced threats like zero-day exploits garner attention in media and academic discourse, the financial sector continues to struggle with more rudimentary but effective attack strategies, such as social engineering and unauthorized access via outdated systems. The significance lies in demonstrating that high-profile threats do not necessarily eclipse simpler yet potent methods.

5.2 Alignment with Research Objectives

The study's first objective was to identify prevalent cyberattack tactics and trends (RQ1). The five sources collectively confirmed the dominance of phishing, ransomware, and DDoS. They also shed light on less obvious vulnerabilities, such as legacy system exploitation, affirming a multifaceted threat environment.

For the second objective, understanding the impact and risks (RQ2), the studies provided a well-rounded picture of not only the financial and operational fallout but also the reputational damage and long-term trust deficits that follow a breach. Notably, all five sources emphasized how a single security failure could spiral into extended customer attrition and regulatory scrutiny, indicating that the ramifications extend well beyond immediate fiscal losses.

Addressing the third objective—proposing and evaluating strategies for resilient defense (RQ3)—the studies converged on the need for layered security measures. Whether through AI-driven threat detection, encryption, or robust incident response protocols, the emphasis was on an integrated approach that marries technology with proactive human governance. Continuous employee training and stakeholder communication emerged as common recommendations, reinforcing the idea that cybersecurity is not merely a technical challenge but an organizational imperative.

In terms of whether these objectives were successfully met, the direct quotes and empirical findings demonstrate a cohesive response. Each research question received clear evidence from at least one of the included studies, offering both statistical data (e.g., frequency of ransomware incidents) and qualitative insights (e.g., executive testimonies on reputational harm). This synergy indicates that the SLR design was effective in capturing multiple dimensions of the problem.

5.3 Theoretical and Practical Implications

The findings contribute to cybersecurity theory by reaffirming the centrality of socio-technical perspectives, particularly in high-stakes domains like finance. While frameworks like Institutional Theory have long posited that organizational pressures shape policy and practice, the empirical data from these five studies stress how such pressures must be integrated with real-time threat intelligence and adaptive incident response models. This highlights a gap in existing theories, which often underestimate the velocity and sophistication of cyber threats.

Practically, the studies underscore the importance of continuous oversight of third-party relationships, a

dimension often overlooked in classical cybersecurity frameworks. By revealing how vendors or partners become inadvertent entry points for attackers, they reinforce the notion that security boundaries extend beyond an institution's immediate infrastructure. Additionally, these works point to the tangible benefits of AI-driven threat detection, which can proactively identify anomalies before they escalate into major breaches, thus guiding future investments in advanced technologies.

From an organizational standpoint, the implications include a shift in policy and training paradigms. Institutions would be well advised to integrate cybersecurity drills and scenario-based training into their standard operating procedures. Moreover, the emphasis on reputation management and transparent communication with stakeholders in the aftermath of breaches highlights a broader strategic orientation, one that transcends mere technical fixes.

5.4 Limitations of the Current Studies

Despite the valuable insights, certain methodological constraints emerge. Four out of the five studies relied heavily on self-reported data from financial institutions, which could lead to underreporting of breaches or an overemphasis on successful defense measures. This inherent bias suggests a potential gap in capturing the full extent of cyber incidents. Moreover, geographic focus, although varied, was still skewed towards developed markets, leaving questions about the transferability of these findings to emerging economies.

Publication bias also presents a challenge. The systematic review protocol attempted to capture all relevant research, but certain high-impact internal reports or industry white papers might not have been published in scholarly databases. As a result, the final pool of studies might not reflect the complete spectrum of real-world scenarios. Lastly, while each study offered granular insights, the small sample size (only five studies) naturally constrains the capacity to generalize. Future research could address these limitations by incorporating a more diverse data set and exploring longitudinal changes in threats and responses.

Ultimately, these findings affirm the pressing importance of integrating socio-technical measures and organizational readiness to combat cyber threats effectively. In doing so, they set the stage for deeper exploration into how financial institutions can evolve from reactive compliance to proactive resilience, thereby safeguarding their critical assets, consumer trust, and operational continuity.

VI. RECOMMENDATIONS FOR PRACTICE

6.1 Strategic Recommendations for Financial Institutions

To enhance cybersecurity resilience, financial institutions should adopt a layered security approach. This involves integrating multiple defense mechanisms such as firewalls, intrusion detection systems, encryption, and endpoint protection to create overlapping security barriers (Uchenna et al., 2021). Additionally, establishing a robust cybersecurity culture is paramount. Institutions must invest in continuous staff training programs that emphasize the importance of security awareness and the role each employee plays in safeguarding digital assets (Georgiadou et al., 2022). Regular drills and scenario-based training can reinforce best practices and prepare staff to respond effectively to potential threats.

6.2 Policy and Regulatory Considerations

Strengthening coordination among government bodies and regulatory agencies is essential to create a unified defense against cyber threats. Policymakers should collaborate to develop comprehensive regulatory frameworks that address emerging vulnerabilities, particularly those associated with third-party service providers and legacy systems (D'Arcy and Basoglu, 2022). Enhancements to existing regulations, such as incorporating requirements for real-time threat intelligence sharing and mandatory incident reporting, can significantly improve the sector's overall security posture.

6.3 Future Research Directions

Future research should extend the systematic literature review to encompass emerging technologies like the Internet of Things (IoT) and quantum computing, which present new cybersecurity challenges and opportunities (Darem et al., 2023). Additionally, empirical studies, including detailed case studies and

longitudinal research, are recommended to provide deeper insights into the effectiveness of various resilience strategies over time. Such research can help in understanding the dynamic nature of cyber threats and the evolving defense mechanisms required to counter them effectively.

CONCLUSION

7.1 Summary of Key Insights

This systematic literature review has identified prevalent cyberattack vectors such as phishing, ransomware, and DDoS attacks within the financial sector. It has also highlighted the significant risks these threats pose, including financial losses, reputational damage, and operational disruptions. Furthermore, the review underscored the necessity of robust defense strategies, combining technical controls with organizational practices to achieve resilience.

7.2 Contributions to Literature and Practice

This SLR advances the understanding of cyber threats in finance by consolidating empirical findings and theoretical frameworks that emphasize a multi-layered defense approach. It provides practical value for financial institutions by outlining effective strategies and best practices that enhance cybersecurity resilience, thereby enabling organizations to better protect their assets and maintain consumer trust.

7.3 Final Remarks and Next Steps

As the cybersecurity landscape continues to evolve, financial institutions must remain vigilant and adaptive. This study calls for increased collaboration between academia, industry, and regulatory bodies to develop innovative security solutions and comprehensive policies. Future efforts should focus on bridging gaps in existing frameworks and fostering a proactive security culture to mitigate emerging threats effectively. By working together, stakeholders can bolster the financial sector's defenses, ensuring its stability and integrity in an increasingly digital world.

REFERENCES

[1] Acar, A., Lu, L., Uluagac, A.S. and Kirda, E., 2019. An analysis of malware trends in enterprise networks. In *Information Security: 22nd International Conference, ISC 2019, New York City, NY, USA, September 16–18, 2019, Proceedings 22* (pp. 360-380). Springer International Publishing.

[2] Ahmad, A.S., 2023. Application of Big Data and Artificial Intelligence in Strengthening Fraud Analytics and Cybersecurity Resilience in Global Financial Markets. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *7*(12), pp.11-23.

[3] Al-Alawi, A.I. and Al-Bassam, M.S.A., 2020. The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), pp.1523-1536.

[4] Böhme, R., Laube, S. and Riek, M., 2019. A fundamental approach to cyber risk analysis. *Variance*, *12*(2), pp.161-185.

[5] Darem, A.A., Alhashmi, A.A., Alkhaldi, T.M., Alashjaee, A.M., Alanazi, S.M. and Ebad, S.A., 2023. Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, *11*, pp.125138-125158.

[6] D'Arcy, J. and Basoglu, A., 2022. The influences of public and institutional pressure on firms' cybersecurity disclosures. *Journal of the Association for Information Systems*, *23*(3), pp.779-805.

[7] European Union Agency for Cybersecurity (ENISA), 2021. *ENISA Threat Landscape 2021: Cyber Attacks, Threat Actors and Trends.* [online] Available at: https://op.europa.eu/en/publication-detail/-/publication/98368007-475a-11ec-91ac-01aa75ed71a1/language-en [Accessed 26 January 2023].

[8] Georgiadou, A., Mouzakitis, S. and Askounis, D., 2022. Detecting insider threat via a cyber-security culture framework. *Journal of Computer Information Systems*, *62*(4), pp.706-716.

[9] International Organization for Standardization (ISO), 2018. *ISO/IEC 27001 Information Security Management.* [online] Available at: https://www.iso.org/standard/27001 [Accessed 26 January 2023].

[10] Kumari, S. and Farheen, S., 2020, May. Blockchain based data security for financial

transaction system. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 829-833). IEEE.

[11] Mastroeni, L., Mazzoccoli, A. and Naldi, M., 2023. Cyber Insurance Premium Setting for Multi-Site Companies under Risk Correlation. *Risks*, *11*(10), p.167.

[12] Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., Stewart, L.A. and Prisma-P Group, 2015. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic reviews*, *4*, pp.1-9.

[13] Paananen, K.M., 2023. The management of information and cybersecurity and the protection of intellectual capital: a systematic literature review.

[14] Patino, C.M. and Ferreira, J.C., 2018. Inclusion and exclusion criteria in research studies: definitions and why they matter. *Jornal Brasileiro de Pneumologia*, *44*, pp.84-84.

[15] Peihani, M., 2022. Regulation of cyber risk in the banking system: a Canadian case study. *Journal of Financial Regulation*, *8*(2), pp.139-161.

[16] Turskis, Z., Goranin, N., Nurusheva, A. and Boranbayev, S., 2019. Information security risk assessment in critical infrastructure: a hybrid MCDM approach. *Informatica*, *30*(1), pp.187-211.

[17] Uchenna, C.C., Jamil, N., Ismail, R., Yan, L.K. and Mohamed, M.A., 2021. Malware threat analysis techniques and approaches for iot applications: A review. *Bulletin of Electrical Engineering and Informatics*, *10*(3), pp.1558-1571.

[18] Von Solms, B. and Von Solms, R., 2018. Cybersecurity and information security–what goes where?. *Information & Computer Security*, *26*(1), pp.2-9.