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

(RESEARCH ARTICLE)

Check for updates

Advancing Cybersecurity Governance: Adaptive Resilience and Strategic Third-Party Risk Management in Financial Services

Oluwatoyin Funmilayo Ayodele * and Adesola Oluwatosin Adelaja

University of Virginia Darden School of Business, Charlottesville, VA, USA.

World Journal of Advanced Research and Reviews, 2024, 24(02), 293–302

Publication history: Received on 15 September 2024; revised on 27 October 2024; accepted on 29 October 2024.

Article DOI: https://doi.org/10.30574/wjarr.2024.24.2.3312

Abstract

As cyberattacks increase, banks and financial firms face new challenges. This research aims to improve cybersecurity by integrating adaptive resilience and strategic third-party risk management into current systems. This study uses thorough qualitative research methods to assess existing frameworks, identifying shortcomings that put companies at more risk. Findings reveal that firms using adaptive resilience - where governance policies adjust with real-time threat information and post-incident evaluation after incidents are much better at preventing and addressing cyber attacks. This paper stresses the importance of including third-party risk management in a comprehensive governance framework, as weaknesses in these relationships often lead to breaches. This study contributes critical insights and a strategic framework for financial institutions to bolster their defenses against sophisticated cyber threats, ensuring sustained resilience and security.

Keywords: Cybersecurity Governance; Adaptive Resilience; Third-Party Risk Management; Financial Services; Cyber Resilience Strategies

1 Introduction

1.1 The Need for Adaptive Cybersecurity Governance in Financial Services

In modern times, digital innovation is making the financial services sector more and more vulnerable to highly advanced cyber threats. Traditional cybersecurity governance frameworks, which include strategic objectives, processes, and accountability for cybersecurity activities within an organization, primarily focus on regulatory compliance rather than operational resilience. This focus on compliance, while important, is an insufficient response to increasing challenges. Financial institutions are increasingly recognizing the need for a paradigm shift towards more dynamic governance models that prioritize adaptive resilience—an approach centered on continuous improvement and real-time threat intelligence—and strategic third-party risk management to alleviate the risks linked to external vendors and partners.

Cybersecurity has emerged from being a technical issue to a highly strategic problem that demands top leadership attention in financial institutions. These institutions have become main targets for sophisticated cyber attacks because of their increased dependence on digital infrastructure and access to significant volumes of sensitive data. Cyber disasters, e.g., the widespread ransomware attack that encrypted data across global networks and demanded ransom payments, have underlined the weaknesses of static governance frameworks. These models often struggle to adjust to the rapidly evolving threat landscape, underscoring the need for more dynamic and resilient cybersecurity frameworks that can tackle emerging threats. It therefore requires an approach whereby the cybersecurity governance framework becomes adaptive with resilience through continuous updating and revision of controls based on real-time threat intelligence and post-incident analysis. This plan is compliant with regulatory requirements and adopts a more proactive stance against the threats. In addition to the fact that financial institutions are increasingly involving third-

* Corresponding author: Oluwatoyin Funmilayo Ayodele

party providers in their operations, setting up effective third-party risk management systems would be very fundamental. Research has shown that a significant portion of cybersecurity vulnerabilities stems from third-party risks, making comprehensive risk management strategies critical in mitigating these risks and ensuring institutional resilience [FSB, 2023].

This research aims to improve the understanding of cybersecurity governance in financial services by evaluating existing models, exploring the benefits of incorporating adaptive resilience and third-party risk management, and suggesting a new governance framework that enhances both security and resilience. Transitioning from a compliance-oriented to a proactive strategy enables financial institutions to improve operational protection, sustain stakeholder confidence, and secure long-term resilience within an increasingly complex cyber environment.

1.1. Fundamental Constructs in Cybersecurity Governance: An Overview

To establish a solid foundation for subsequent discussions in this paper, it is essential to accurately define and clarify the key concepts pertinent to this study. The subjects include cybersecurity, cybersecurity governance, adaptive resilience, and third-party risk management. Understanding the terminology within the financial services sector is crucial for grasping the methods and frameworks analyzed in this research.

Cybersecurity encompasses the policies and procedures designed to protect digital infrastructures, networks, and sensitive data from unauthorized access, attacks, or destruction. It covers a wide area of technologies and strategic methods for information protection in a manner that will not violate the confidentiality, integrity, and availability of it. In the financial services sector, where institutions handle large amounts of sensitive data and rely heavily on digital infrastructure, robust cybersecurity is essential. Financial institutions face several cyber threats, such as data breaches, ransomware, and phishing attacks, which can result in considerable financial and reputational damage. Effective cybersecurity governance involves the implementation of technological measures—such as firewalls, encryption, and intrusion detection systems—alongside comprehensive policies, regular staff training, and a strategic incident response framework.

Cybersecurity governance serves as the framework through which an organization directs and oversees its cybersecurity efforts. It involves the development of policies, methodologies, and frameworks to ensure cybersecurity activities align with the organization's strategic objectives and regulatory requirements. In the financial services sector, cybersecurity governance is crucial owing to the substantial risks involved in managing and protecting sensitive financial information. Effective governance ensures clear accountability at the senior management level, appropriate resource distribution, and continuous evaluation and oversight of cybersecurity protocols. Cybersecurity includes ensuring compliance with critical business regulations and standards, e.g., General Data Protection Regulation (GDPR) and the New York Department of Financial Services (NYDFS) Cybersecurity Regulation. Incorporating cybersecurity into the comprehensive governance framework allows organizations to manage risks more efficiently, enhance defensive strategies, and ensure sustained operational resilience. This integration aids institutions in meeting regulatory requirements while actively addressing emerging cyber threats through a more systematic and strategic risk management approach.

Adaptive resilience involves the ability of an organization to anticipate, plan for, mitigate, and return to full functionality after cyber disasters with as little disruption as possible. Unlike traditional models of resilience, which are primarily aimed at recovery after incidents, adaptive resilience will pay more attention to continuous improvements and rapid adaptation to emerging risks. This is particularly critical in the financial service sector, as the growing sophistication of cyber threats may have serious consequences on operational stability and trust. An organization that is adaptively resilient stands out in its ability to detect threats much earlier, react faster, and recover effectively, thereby reducing the overall impact of cyber catastrophes. To achieve this, institutions need to implement governance models that incorporate real-time threat intelligence, continuous monitoring, and post-incident analyses to dynamically refine and enhance their security strategies [BCI, 2023; EY, 2023].

Third-party risk management (TPRM) is vital in the financial services industry owing to the increasing reliance on external vendors for critical operations, including IT infrastructure, cloud computing, and payment processing. External contacts subject enterprises to cybersecurity risks, since other parties may get access to sensitive information or essential systems. A robust TPRM strategy requires thorough due diligence in vendor selection, ongoing monitoring of third-party activity, and the enforcement of stringent security standards to guarantee adherence to the financial institution's cybersecurity regulations. The ongoing advancement of cyber threats requires a robust Third-Party Risk Management (TPRM) framework to address the risks associated with data breaches and operational disruptions, which are increasingly common due to weaknesses in third-party systems.

1.2. Evolution of Cybersecurity Governance in Financial Services

The development of cybersecurity governance in financial services has been profoundly shaped by the substantial growth of the sector over the years, driven by digitalization and the incorporation of technologies such as online banking, mobile payments, and digital financial products. These enhancements have expanded the attack surface, making institutions susceptible to increasingly sophisticated cyber attacks. As financial services grow more interconnected, the potential ramifications of hacks have escalated, making robust cybersecurity governance more critical than ever. The growing interconnectivity of financial institutions and their ecosystems necessitates adaptive and resilient cybersecurity strategies to manage the associated risks.

The cybersecurity governance related to financial services traditionally has been directed toward making sure that compliance is adhered to, wherein the institutions concerned focus on adherence to regulatory requirements, including the General Data Protection Regulation in Europe and the Cybersecurity Regulation of the New York Department of Financial Services (NYDFS) in the United States. This compliance-centric strategy has led to inconsistencies among regulatory standards and companies' abilities to protect against increasingly complex cyber threats. The adoption of more comprehensive cybersecurity practices, including continuous monitoring and adaptive incident response frameworks, is critical to bridging the gap between compliance and operational resilience in the face of evolving threats [FSB, 2020].

1.3. Theoretical Foundations of Cybersecurity Governance

The governance of cybersecurity in financial services is informed by contemporary concepts that establish a framework for managing and mitigating cyber attacks. At the core of this discussion is Cybersecurity Governance Frameworks and Modern Organizational Resilience, specifically emphasizing third-party risk management. Cybersecurity governance frameworks have evolved considerably to address the intricate and dynamic characteristics of cyber threats within the financial industry. Frameworks like the NIST Cybersecurity Framework emphasize the imperative for an integrated approach that aligns cybersecurity activities with the core objectives of the organization. These frameworks are designed to help institutions not only meet regulatory requirements but also adapt to emerging threats through continuous improvement and real-time threat intelligence [NIST, 2024]. The critical integration of cybersecurity risk management into broader strategic management processes is highlighted by Mizrak (2023), emphasizing that effective governance must be both proactive and adaptive to remain relevant in the face of evolving threats. A vital aspect of this governance is the management of third-party risks, in which frameworks must ensure that external suppliers adhere to the institution's rigorous cybersecurity standards.

The notion of contemporary organizational resilience has gained more relevance in the domain of cybersecurity governance, particularly for financial institutions. This concept asserts that organizations must not only prepare for and recuperate from cyber incidents but also have the capacity to consistently adapt to and manage them. Resilience involves not just rehabilitation efforts but also requires proactive measures to ensure the continuous functioning of critical systems and operations, notwithstanding persistent and evolving cyber threats.

A crucial element of resilience-focused solutions is the adept handling of third-party risks, as vulnerabilities disruptions in the supply chain or external partnerships may severely undermine an institution's ability to maintain uninterrupted operations during a cyber attack. Thus, organizational resilience demands a comprehensive approach, one that integrates both internal and external risk management to safeguard operational continuity in the face of cyber threats (Mizrak, 2023).

1.4. Challenges and Barriers in Implementing Cybersecurity Governance

Implementing robust cybersecurity governance in financial institutions is fraught with challenges, despite the clear benefits of such frameworks. One of the most significant challenges is balancing the need for regulatory compliance with the imperative for operational resilience. Regulatory frameworks, e.g., the General Data Protection Regulation (GDPR) in Europe and the New York Department of Financial Services (NYDFS) Cybersecurity Regulation in the United States, establish strict standards for data protection and cybersecurity practices. While these regulations are crucial for ensuring a baseline level of security, they often lead institutions to adopt a compliance-focused approach. This focus on compliance, sometimes referred to as a "checkbox" mentality, can prioritize meeting regulatory requirements over developing systems that are genuinely resilient. Such an approach can limit an institution's ability to respond dynamically to emerging threats, as it emphasizes adherence to static rules rather than fostering a culture of continuous improvement and adaptability. The 2023 amendments to the NYDFS Cybersecurity Regulation encourage a shift toward dynamic, risk-based cybersecurity practices. These updates emphasize continuous monitoring, real-time risk assessments, and proactive threat management to better protect against evolving cyber risks (NYDFS, 2023).

Obi et al. (2024) underscores the complexity of modern cybersecurity threats, including ransomware and insider attacks, which require financial institutions to adopt more proactive strategies. Savaş and Karataş (2022) advocate for a globally aligned cybersecurity governance model that emphasizes transparency, accountability, and inclusivity, involving both public and private sectors. They argue that a collaborative approach, incorporating international standards, can help institutions move beyond rigid compliance and focus on resilience and adaptability. This is particularly crucial in the modern integrated financial industry, where cybersecurity threats sometimes transcend national boundaries and require coordinated responses.

The fact that cybersecurity governance frameworks have not been widely established so far is mainly related to the issue that such initiatives come at substantially high costs. Establishing and sustaining a resilient cybersecurity framework requires significant investments in both monetary and human capital. This regulation may provide challenges for some businesses, especially smaller entities. The costs related to acquiring cybersecurity solutions, conducting ongoing threat monitoring, providing personnel training, and ensuring regulatory compliance can strain budgets. This often leads some institutions to adopt a reactive rather than proactive approach to cybersecurity, making them more vulnerable to emerging threats (Uzougbo et al., 2024).

The complexity of third-party risk management (TPRM) is a further hurdle. As financial institutions' dependence on external sources grows, the management of associated risks becomes even more intricate. Effective third-party risk management requires institutions to do thorough due diligence on their contractors, ensuring adherence to rigorous cybersecurity standards. Nevertheless, the complexity of supply chains and the constantly evolving complexity of vendor relationships can hinder the achievement of comprehensive monitoring. Continuous monitoring and reassessment of third-party risks are essential to ensure they do not compromise the institution's overall cybersecurity posture (HelpNetSecurity, 2024).

These challenges are further exacerbated by the constantly changing landscape of cyber threats. This implies that new, sophisticated attacks are developing at a pace never seen before, and financial institutions have to invariably keep pace with them by adjusting to cybersecurity protocols and strategies. The swift advancement of technologies like artificial intelligence (AI) and machine learning (ML) has enabled attackers to create more complex and targeted cyberattacks. Concurrently, the intensification of the intricacy of financial systems and the global interdependence of financial markets make it difficult for institutions to foresee and protect against all potential attacks. Developing cybersecurity frameworks that are both robust and adaptable is critical in ensuring that institutions remain resilient against the ever-changing nature of cyber threats (Oyeniyi et al., 2024).

Finally, Cultural and organizational barriers may impede the effective implementation of cybersecurity governance frameworks. Nobles (2020) highlights the issue of security fatigue, where constant security demands lead to cognitive overload, reducing compliance and increasing errors. This highlights the imperative for a human-centered approach programs that integrate regular training and workload assessments to mitigate these risks. Furthermore, top leadership often regards cybersecurity as a technical issue rather than a strategic one leading to inadequate investment in resilience-focused frameworks and fragmented systems that hinder effectiveness conveyance of information. Overcoming these barriers requires integrating cybersecurity into strategic management (Enisa, 2018; Mani, 2021).

1.5. Research Gaps and Future Directions in Adaptive Resilience and Third-Party Risk Management

A significant deficiency is seen in the insufficient integration of adaptive resilience within existing governance frameworks. While the concept is receiving attention, its practical integration into cybersecurity governance frameworks persists and needs to be more adequately scrutinized. Contemporary research often highlights resilience in certain circumstances, such as disaster recovery or business continuity; however, it fails to examine how financial institutions may incorporate real-time threat intelligence with continuing operations improvement within their corporate governance systems. Research is necessary to examine the systematic incorporation of adaptive resilience across all tiers of governance, from policy development to operational execution.

Although TPRM is recognized as a crucial component of cybersecurity, a substantial segment of the literature discusses it as a standalone function rather than an integrated element of resilience strategies. There is limited research on how organizations can monitor and manage, in real time, third-party risks concurrently with their own evolving threat landscape. This gap is even more significant for financial services companies because the firms normally contract services through complex networks of third-party service providers, further increasing their susceptibility to cyber attacks.

Furthermore, challenges remain in the formulation of explicit criteria for performance assessment methods for adaptive resilience and third-party risk management. While several models exist for assessing generic cybersecurity threats, few provide practical, quantitative indicators on the effectiveness of institutional responses to management of threats or third-party attacks. The findings of this research will enable firms to reassess their strategies and introduce evidence-based improvement

1.6. Prospective Developments in Adaptive Resilience and Third-Party Risk Management

Future research should focus on creating comprehensive frameworks that include adaptive resilience in governance models for financial institutions. These frameworks must include continuous monitoring, incorporate real-time threat intelligence and flexible response strategies into standard operations. Moreover, the frameworks must exhibit flexibility, enabling institutions to adapt their governance models in reaction to evolving dangers and technological advancements. Aligning resilience strategies with regulatory mandates will be essential for guaranteeing compliance without sacrificing operational agility.

The development of artificial intelligence (AI) and machine learning (ML) holds the potential to change third-party risk management. The increasing complexity of third-party networks requires automated solutions that can monitor and mitigate threats in real time. AI-driven tools can reliably monitor vendor behavior, detect potential security concerns, and provide automated alerts to organizations before vulnerabilities are exploited. Moreover, further study should examine the role of blockchain technology in enhancing transparency and obligations of external vendors.

Future research should integrate principles from behavioral science, risk management, and technology to provide a thorough understanding of how organizations may adjust and protect themselves from external threats. Collaborative efforts across academia, industry, and government can produce critical insights for the formulation of innovative solutions, governance frameworks that are resilient and flexible to current and future threats.

The progression of real-time, cloud-based risk management solutions is crucial. These platforms should let financial institutions simultaneously monitor internal cybersecurity processes and third-party safeguard risks, necessitating a comprehensive and coherent plan for management. Future research should focus on the secure and effective large-scale deployment of these systems, with particular emphasis on establishing equilibrium innovation alongside regulatory compliance.

1.7. Technological Innovations for Enhancing Cybersecurity Governance

Technological innovations are crucial for improving cybersecurity frameworks, particularly as cyber threats are becoming intricate and pervasive. In the domain of financial services, the integration of advanced technologies like Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Regulatory Technology (RegTech), Third-Party Risk Management (TPRM) systems, and Threat Intelligence Platforms (TIPs) is crucial for developing resilient and flexible security solutions. These advancements aid institutions in mitigating cyber attacks through the proactive identification of vulnerabilities, management of third-party risks, and assurance of regulatory compliance.

Bokhari and Myeong (2023) analyze the effect of AI on cybersecurity in smart cities, demonstrating that AI can enable real-time threat detection, automate responses, and support continuous system enhancements. When applied to financial services, this approach could empower institutions to swiftly identify and respond to emerging cyber threats. AI also bolsters data security by ensuring that access is limited to authorized users, a critical factor as financial systems grow increasingly interconnected.

Bello et al. (2023) emphasize the transformative potential of integrating ML and AI into fraud detection systems. These technologies enable financial institutions to analyze vast datasets in real time, improving their ability to detect and respond to suspicious activities proactively. Furthermore, the incorporation of advanced defense strategies, such as intrusion detection systems and behavior analytics, strengthens the overall security posture of these organizations.

Abrahams et al. (2024) emphasize the importance of evolving cybersecurity strategies that incorporate AI-driven tools alongside effective human engagement. This human-centric approach to AI in cybersecurity highlights that technology alone is insufficient for safeguarding critical data, underscoring the need for a balanced strategy that includes awareness and training programs. Integrating these advanced tools, along with international policy standards, could further enhance adaptive resilience by aligning both technological and human-focused measures across governance frameworks.

AI and Machine Learning are modifying the way financial organizations can respond to, or even detect, cyber threats. According to the Ponemon Institute, organizations that implement AI and automated security systems are in a position to mitigate and minimize the time taken to detect or respond to such a breach. By automating the processes for detection and response to threats, AI improves an institutional capability for adaptation to evolving risks by embedding adaptive resilience into the governance framework. (Ponemon Institute, 2019).

Blockchain technology can help in making financial services not only secure but more transparent. Its decentralized nature ensures that once data is recorded, it cannot be altered, making it a powerful tool for preventing tampering and securing sensitive information. It's particularly well suited to third-party risk management because blockchain allows real time monitoring of vendor activities and maintains an immutable record of transactions. Additionally, blockchain can automate compliance checks using smart contracts, further improving operational efficiency and trust between institutions and their vendors (FTI Technology, 2023).

RegTech solutions are increasingly important to financial institutions working to stay in compliance with ever changing regulations and also enhance their cybersecurity. Artificial intelligence (AI) and big data analytics help RegTech platforms monitor transactions, assess risk and streamline compliance processes. These technologies enable institutions to meet regulatory requirements while remaining agile in their response to emerging threats, thus supporting a more proactive cybersecurity governance model (Abikoye et al., 2023).

Third-Party Risk Management (TPRM) platforms are the means of continuously monitoring and managing the cybersecurity posture of external vendors. With the help of AI and automation, these platforms are able to assess in real time the risk posed by third-party providers, so that financial institutions are able to identify and address risks throughout their supply chains before such terms are exploited. Yang (2019) emphasizes that effective big data governance is crucial for enhancing the security of data shared with third parties, further supporting the need for robust TPRM practices. As financial institutions increasingly rely on third-party services, they must strengthen their TPRM capabilities to mitigate the risks emerging from these vendor relationships. This approach not only addresses security gaps but also ensures resilience in the face of evolving cyber threats (McKinsey, 2023).

Threat Intelligence Platforms (TIPs) are platforms that aggregate and analyze data from multiple sources in real time to give an organization insights into potential or impending cyber threats. Financial institutions can advance beyond the reactive security stance and instead work to prevent emerging (and unknown) risks by integrating TIPs into their cybersecurity governance frameworks. TIPs also facilitate collaboration with external partners and industry groups, enhancing the collective defense against sophisticated attacks (Ponemon Institute, 2019).

As the landscape of threats evolve, the strategic deployment of AI, blockchain, RegTech, TPRM platforms, and TIPs will be crucial in ensuring that governance frameworks are both resilient and adaptive, allowing financial institutions to meet regulatory standards while effectively protecting against future threats (KPMG, 2021).

1.8. Objectives and Scope of the Current Research

This research focuses on exploring and proposing a comprehensive cybersecurity governance framework within the financial services sector, which integrates adaptive resilience and third-party risk management. This research seeks to address the following specific objectives:

- Critically evaluate the current cybersecurity governance models by taking into consideration the available cybersecurity governance frameworks applied within the financial services industry to identify weaknesses and strengths, and any further scope for improvement in light of fast-changing cyber threats and reliance on third-party vendors
- Discuss the concept of adaptive resilience, considering how this can be inculcated into the governing models currently applied to organizational responses and recoveries from cyber incidents
- Analyze different challenges that third-party risk management poses to the betterment of cybersecurity governance and how those challenges can be mitigated by the identification of effective strategies toward the inclusions of third-party risk management into the governance framework
- Explore technological innovations that can enable adaptive resilience and third-party risk management under governance frameworks such as AI, Blockchain, RegTech, and other high end technologies
- Develop a new, integrated cybersecurity governance framework to address the shortcomings of the current models in a manner that adaptive resilience and third-party risk management are integrated to leverage technological innovations, toward the pursuit of an enhanced overall cybersecurity posture of financial institutions.

This research is limited to the financial services sector and specifically, those institutions that, beyond their payments business, are highly dependent on their digital infrastructure and on third-party vendors. The study is predominantly going to draw from recent literature and industry reports of the past five years to ensure the findings and recommendations are meaningful in today's cybersecurity landscape. On the other hand, research will also consider regulatory frameworks such as the GDPR and the NYDFS Cybersecurity Regulation, to analyze how these regulatory requirements dictate financial institution's cybersecurity governance. However, the scope does not include other sectors, and results cannot necessarily be transferred to other industries.

This research seeks to make a contribution to the academic and professional discourses in cybersecurity governance by delivering a framework covering the regulatory requirements, yet one that reinforces the resilience and security of financial institutions against future cyber threats.

2. Research Methodology

2.1. Approach

This study adopts a qualitative research approach, with a focus on in-depth analysis of literature reviews and industry reports. The research methodology includes the following steps:

Literature Review: The research begins with an extensive literature review to establish a theoretical foundation for the study. Academic journals, industry reports, and case studies published within the last five years are analyzed to understand the current state of cybersecurity governance in the financial services sector. The literature review focuses on identifying gaps in existing frameworks, particularly regarding adaptive resilience and third-party risk management. Key concepts, such as cybersecurity governance frameworks, resilience theory, and technological innovations, are critically examined to provide a context for the research.

Expert Opinions: While no direct interviews were conducted, the study relies on published expert opinions and analyses in industry reports, white papers, and academic articles. These sources provide valuable insights into the current state of cybersecurity governance and thus become necessary to turn with a dynamic threat environment.

Framework Development: Through the literature review and expert views, a new cybersecurity governance framework has been developed in the current study. The proposed framework is more dynamic and adaptive.

3. Results and discussion

This study's findings support the implementation of adaptive resilience and TPRM within cybersecurity governance frameworks in the financial services sector. This research undertakes an examination of pertinent weaknesses of existing governance models through a critical review of existing literature, as well as case studies based on practical experience, as a foundation for advancing a more adaptive and dynamic approach.

3.1. Results: Key Findings

This research reveals the extent to which current cybersecurity governance models within financial institutions tend to be more concerned about regulatory compliance than with true security. Many institutions treat cybersecurity as a tick box exercise of compliance with regulatory requirements including the General Data Protection Regulation (GDPR) and the New York Department of Financial Services (NYDFS) Cybersecurity Regulation. This compliance driven strategy is hugely important but highly limited in its ability to address an ever more complicated and specialized cyber threat. One of the most striking findings is that a compliance first mentality is unlikely to prevent or mitigate a large scale cyber incident. In contrast, those that embraced adaptive resilience (leveraging real-time threat intelligence, continuous monitoring, and post incident analysis) were better able to respond to and recover from the cyber incident. The results indicate that adaptive resilience not only provides organizations with enhanced abilities to resist attacks, but it also drives the shaping of central governance strategies to adapt and overcome novel and ever changing threats.

The research also shows that in many institutions, third-party risk management (TPRM) is an underdeveloped area. Even financial organizations depend on third parties in terms of networks of vendors and service providers, and many of them fail to continuously assess security postures of these third parties. These vulnerabilities are being left open by this oversight and easy to exploit by attackers.

3.2. Proposed Cybersecurity Governance Framework

This research then proposes a comprehensive cybersecurity governance framework specifically for financial institutions based on these findings. It resolves compliance focused models' limitations by integrating TPRM with adaptive resilience in a unified governance structure.

Adaptive Resilience Core: This framework is underpinned by adaptive resilience which means that institutions continually monitor threats and revise their security accordingly as new threats arise. The use of AI enabled tools for real time threat detection reduces the time required to detect and respond to breaches thereby improving the way institutions evolve their security strategy based on instantaneous changes in threats. Financial institutions can move from reactive to proactive, adaptive. Yang (2019) highlights that well-governed big data can significantly contribute to advanced threat detection and response capability, enabling organizations to use advanced analytics for better situational awareness. Furthermore, Tagarev (2020) emphasizes that collaborative governance, involving both public and private sectors, enhances resilience by fostering shared goals and transparent communication. To further enhance resilience, Mulugeta (2023) proposes a dynamic governance model that incorporates real-time risk identification, strategic resource allocation, and adaptability to evolving threats. This framework emphasizes ongoing evaluation and collaboration, supporting resilience by ensuring that financial institutions adapt to shifting cyber threats through public-private partnerships, performance metrics, and compliance frameworks

Third-Party Risk Management Integration: TPRM is also fully integrated into the framework, treating the third-party risks as critical as the internal risks. McKinsey noted that third-party risk management needs to be taken proactive in order to ensure cybersecurity resilience given the growing reliance on cloud services and other third-party technologies. Real time monitoring and automation enable institutions to address those vulnerabilities in real time, minimizing their exposure to external supply chain attacks. As emerging technologies and evolving threats reshape the financial services industry, integrating TPRM into governance frameworks ensures that institutions remain agile and well-prepared for future challenges (McKinsey, 2023).

Regulatory Compliance as a Baseline: Compliance with frameworks such as GDPR and NYDFS sets a foundational layer for cybersecurity governance within financial institutions. While these regulations establish essential security standards, they are not sufficient for addressing the evolving cyber threat landscape. Yusif and Hafeez-Baig (2021) argue that a comprehensive governance model should go beyond static regulatory compliance, incorporating real-time monitoring and continuous improvement to respond dynamically to emerging threats. This alignment of cybersecurity with broader governance goals enables institutions to meet regulatory requirements while proactively adapting to potential risks, moving from a compliance-centric model to one of strategic, adaptive resilience.

Incorporation of Threat Intelligence Platforms (TIPs): The framework integrates TIPs, which give real-time feeds to the institution over active threats. TIPs aggregate data from multiple sources, offering a comprehensive view of the threat landscape. This allows financial institutions to anticipate risks and adjust their security measures accordingly, making TIPs a crucial tool for proactive cybersecurity governance (Ponemon Institute, 2019).

Standardized Metrics for Continuous Improvement: Evaluation of performance is one of the critical gaps identified in cybersecurity governance and the lack of standardized metrics to be evaluated. Like the insights gained from analyzing the performance of internal cybersecurity measures - the time it takes to detect and respond to incidents, the rate at which third-party risks are mitigated, and the frequency at which governance updates are delivered. They allow financial institutions to measure their adaptability and the capacity to address growing cyber threats. As financial institutions begin to adopt new technologies e.g., cloud computing and Artificial Intelligence (AI), McKinsey stresses that financial institutions must enhance their cybersecurity capabilities, including continuous processes and real time assessments to responsibly manage the increased risks exposed by these technologies, these capabilities are critical to — for example — managing third-party risks, privilege access, as well as securing the data. McKinsey notes that without improving these critical areas, financial institutions risk falling behind in safeguarding their assets and customers against cyber threats (McKinsey, 2023).

3.3. Challenges in Implementing the Framework

While the proposed framework is, no doubt, comprehensive, the path to its execution is beset with challenges. Cost acts as the major impediment; after all, AI-driven tools and TIPs require huge investments that might prove very expensive for smaller institutions. Moreover, the organizational culture in most financial institutions relegates cybersecurity to just a technical issue, rather than a strategic one. Overcoming these cultural barriers requires a shift in mindset at the leadership level, where cybersecurity governance is viewed as essential to the institution’s overall resilience (Mani, 2021).

3.4. Future Research Directions

This study develops a strong governance framework, but more future research is necessary to explore the reality of this model's practical application in other types of financial institutions, especially those smaller organizations that may have resource constraints. Moreover, future research should be directed to develop universally applicable criteria pertaining to the performance evaluation of adaptive resilience and TPRM strategies. Lastly, along with the innovation of technologies like AI and blockchain, more research should explore their potential to help improve cybersecurity governance by automating risk management processes in very risky fields such as the financial sector.

4. Conclusion

The increasingly sophisticated nature and volume of cyber threats in financial services do indeed call for a movement away from compliance-based cybersecurity toward more flexible approaches. This research illustrates how existing frameworks, though useful in facilitating compliance with regulations, are not well adapted to threats that keep evolving. Results indicate that organizations embracing adaptive resilience - always watching, preventing and learning from cyber threats - handle operational security better and restore functions after incidents faster.

The study also points out how vital Third-Party Risk Management (TPRM) is for keeping the extended enterprise safe. As financial services rely more on outside partners, strong TPRM plans should become part of governance systems. Using AI-powered TPRM tools and regular vendor checks is necessary to reduce risks.

This study suggests a full cybersecurity plan that combines adaptable resilience, TPRM and regulatory compliance into one model. This plan uses new technologies like Artificial Intelligence (AI), Machine Learning (ML), Threat Intelligence Platforms (TIPs) and blockchain. However, the implementation of this framework comes with challenges, particularly related to costs and organizational culture. Smaller financial institutions may have limited resources. However, a large number of institutions are compelled to shift their policies on cybersecurity from a technical problem to a strategic issue integrated into all levels of governance.

The research thus contributes valuably to future cybersecurity governance in the financial services sector as it provides an action-oriented framework that is targeted at addressing the identified key challenges. The proposed framework underlines continuous adaptation, real-time threat intelligence, and proactive management of internal and external risks beyond mere static models of compliance. It would be at the very core of the adoption of this framework to ensure that long-term resilience and security exist within a financial institution as cyber threats evolve.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abikoye, B.E., Umeorah, S.C., Adelaja, A.O., Ayodele, O., & Ogunsuji, Y.M. (2023). Regulatory compliance and efficiency in financial technologies: Challenges and innovations. Journal of Financial Regulation, 12(4), 85-97.

[2] Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and Effectiveness of Cybersecurity Measures for Data Protection. Computer Science & IT Research Journal, 5(1), 1-25. https://doi.org/10.51594/csitrj.v5i1.699

[3] Bello, O. A., Folorunso, A., Onwuchekwa, J., & Ejiofor, O. E. (2023). A Comprehensive Framework for Strengthening USA Financial Cybersecurity: Integrating Machine Learning and AI in Fraud Detection Systems.

[4] BCI. (2023). The BCI Launches Cyber Resilience Report 2023. Retrieved from https://www.thebci.org/news/the-bci-launches-cyber-resilience-report-2023.html

[5] Bokhari, S. A. A., & Myeong, S. (2023). The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective. IEEE Access, PP(99), 1-1. DOI: 10.1109/ACCESS.2023.3293480. Licensed under CC BY-NC-ND 4.0.

[6] Enisa. (2018). Cybersecurity cultures in organizations. European Union Agency for Cybersecurity. Available from: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

[7] EY. (2023). Building Resilience: Safeguarding Financial Institutions from Modern Cyber Threats. Retrieved from https://www.ey.com/en_ch/cybersecurity/building-resilience-safeguarding-financial-institutions-from-modern-cyber-threats

[8] Financial Stability Board [2020]. Effective Practices for Cyber Incident Response and Recovery. Retrieved from https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery.

[9] FSB. (2023). FSB Publishes Toolkit for Enhancing Third-Party Risk Management and Oversight. Financial Stability Board. Retrieved from https://www.fsb.org/2023/12/fsb-publishes-toolkit-for-enhancing-third-party-risk-management-and-oversight/.

[10] FTI Technology. (2023). Revolutionizing Third-Party Risk Management with Blockchain Technology. Available from: https://www.ftitechnology.com/resources/white-papers/revolutionizing-third-party-risk-management-with-blockchain-technology

[11] HelpNetSecurity. (2024). Third-party risk management: Best practices. Available from: https://www.helpnetsecurity.com/2024/01/29/tprm-best-practices/.

[12] KPMG. (2021). Building resilience in an interconnected world. KPMG Report. https://kpmg.com/us/en/articles/2024/building-resilience-hyperconnected-world.html

[13] Mani, V. (2021). Demystifying the implementation of cyber resilience programs. ISACA Journal, 3(1), 19-23.

[14] McKinsey & Company [2023]. The Cyber Clock Is Ticking: Derisking Emerging Technologies in Financial Services. Retrieved from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services.

[15] Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: A comprehensive literature review. Research Journal of Business and Management, 10(3), 98-108.

[16] Mulugeta, H. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. Journal of Cybersecurity and Privacy, 3(3), 327-350. https://doi.org/10.3390/jcp3030017

[17] NIST. (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology. Available from: https://doi.org/10.6028/NIST.CSWP.29.

[18] New York Department of Financial Services (NYDFS) [2023]. 2023 Amendments to the NYDFS Cybersecurity Regulation. Retrieved from https://www.dfs.ny.gov/system/files/documents/2023/12/rf23_nycrr_part_500_amend02_20231101.pdf.

[19] Nobles, C. N. (2020). Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity. Proceedings of the Fourteenth Midwest Association for Information Systems Conference, Oshkosh, Wisconsin, May 21-22, 2019.

[20] Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. (2024). COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES.

[21] Oyeniyi, L. D., Ugochukwu, C. E., & Mhlongo, N. Z. (2024). Developing Cybersecurity Frameworks for Financial Institutions: A Comprehensive Review and Best Practices. Retrieved from https://doi.org/10.51594/csitrj.v5i4.1049.

[22] Ponemon Institute. (2019). 2019 Cost of a Data Breach Report. Ponemon Institute. Retrieved from https://www.ibm.com/security/data-breach.

[23] Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 45-60. https://doi.org/10.1365/s43439-021-00045-4

[24] Tagarev, T. (2020). Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives. Future Internet, 12(4), 62. https://doi.org/10.3390/fi12040062

[25] Uzougbo, N. S., Ikegwu, C., Adewusi, A. O., & Adewusi, A. O. [2024]. Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. International Journal of Science and Research Archive, 12(01), 533-548. DOI: 10.30574/ijsra.2024.12.1.0802.

[26] Yang, L. (2019). Towards Big Data Governance in Cybersecurity. Data-Enabled Discovery and Applications, 3(1). DOI: 10.1007/s41688-019-0034-9. Licensed under CC BY 4.0.

[27] Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. Journal of Applied Security Research, 16(4), 1-24. https://doi.org/10.1080/19361610.2021.1918995