European Journal of
Business and Strategic Management
(EJBSM)

"Strategic Risk Management in the Age of Cyber Threats: Implications for Financial Institutions"

Abdimalik Hussein

IPRJB
INTERNATIONAL PEER REVIEWED
JOURNAL AND BOOK PUBLISHING

European Journal of Business and Strategic Management
ISSN 2518-265X (Online)
Vol.10, Issue 4, No.1. pp 1 - 14, 2025

www.iprjb.org

Strategic Risk Management in the Age of Cyber Threats: Implications for Financial Institutions

[1*]Abdimalik Hussein

Strathmore University

Article History

Received 4th March 2025

Received in Revised Form 9th April 2025

Accepted 6th May 2025

Abstract

Purpose: This study sought to investigate strategic risk management in the age of cyber threats implicating financial institutions.

Methodology: The study adopted a desktop research methodology. Desk research refers to secondary data or that which can be collected without fieldwork. Desk research is basically involved in collecting data from existing resources hence it is often considered a low cost technique as compared to field research, as the main cost is involved in executive's time, telephone charges and directories. Thus, the study relied on already published studies, reports and statistics. This secondary data was easily accessed through the online journals and library.

Findings: The findings revealed that there exists a contextual and methodological gap relating to the cyber threats. Preliminary empirical review revealed that financial institutions failed to effectively integrate cybersecurity into their strategic risk management frameworks. Cyber risks were often treated as IT issues rather than strategic concerns, leading to reactive responses and a lack of leadership involvement. The study emphasized the need for a shift in how institutions approach cybersecurity, making it a core part of their overall risk management and strategic planning.

Unique Contribution to Theory, Practice and Policy: The study recommended integrating cybersecurity into enterprise risk management, adopting a proactive approach with real-time threat intelligence, and enhancing cross-departmental collaboration. It called for better employee training, clearer regulatory standards, and public-private partnerships. The study contributed to theory by highlighting cybersecurity as a systemic risk and offered practical steps to improve governance and resilience in financial institutions.

Keywords: *Cybersecurity, Strategic Risk Management, Financial Institutions, Enterprise Risk Management (ERM), Cyber Risk Governance*

JEL codes: *033, G32, G21, D81*

1.0 INTRODUCTION

The concept of risk management in financial institutions has evolved dramatically over the last decade, especially after the 2008 financial crisis exposed systemic flaws in global financial systems. In the United States, risk management strategies have been restructured to incorporate advanced analytics, cyber risk response, and regulatory alignment with the Dodd-Frank Act. A 2021 study found that American financial institutions that implemented enterprise risk management (ERM) frameworks achieved a 13% higher return on equity compared to those that did not (Lundqvist, 2021). This effectiveness is attributed to the use of integrated risk frameworks that enable faster detection and mitigation of financial threats. Moreover, the introduction of the Comprehensive Capital Analysis and Review (CCAR) and Dodd-Frank Act stress tests (DFAST) compelled U.S. banks to build risk buffers, thereby improving the resilience of the sector during crises such as COVID-19. These regulatory-driven mechanisms have transformed the perception of risk from a reactive to a strategic capability.

In the United Kingdom, the financial services sector has embraced risk management as a core component of organizational governance. Post-Brexit regulatory adjustments have led to a greater emphasis on managing geopolitical and currency-related risks. The Bank of England's Financial Policy Committee (FPC) has mandated rigorous stress testing and risk disclosure practices, resulting in improved resilience. A 2022 study highlighted that UK-based banks that deployed dynamic risk modeling techniques showed a 17% lower probability of default during market shocks (Baker & Frame, 2022). Moreover, the UK's Senior Managers and Certification Regime (SM&CR) has strengthened individual accountability for risk, reducing moral hazard and enhancing the quality of internal controls. The integration of operational risk and compliance frameworks into corporate strategies has made risk management not only a compliance requirement but also a competitive advantage.

Japan's financial institutions have long emphasized stability, but the modern wave of digitalization and cyber threats has pressured institutions to upgrade their risk management systems. A 2019 study observed that Japanese banks adopting integrated risk data aggregation as guided by Basel III saw a 22% improvement in risk-adjusted returns (Saito et al., 2019). Furthermore, the Financial Services Agency (FSA) in Japan has encouraged scenario-based risk modeling and capital adequacy simulations to ensure preparedness against black swan events. Despite conservative financial behavior, the risk culture in Japan has been criticized for being compliance-oriented rather than proactive. However, recent developments in cyber resilience programs and AI-based risk analytics show promising enhancements in the effectiveness of Japan's financial risk strategies.

Brazil presents a more volatile landscape in terms of risk, due to its history of economic instability and political uncertainty. Nevertheless, the Central Bank of Brazil has implemented macroprudential tools such as the Liquidity Coverage Ratio (LCR) and the Countercyclical Capital Buffer (CCyB) to bolster the banking system's resilience. A 2020 study found that banks in Brazil that adhered to Basel III guidelines showed a 12% improvement in capital adequacy and a 9% reduction in credit default rates (Gonçalves et al., 2020). Brazilian banks have also invested in ERM tools and FinTech collaborations to mitigate credit, market, and operational risks. The country's pioneering use of risk dashboards and early-warning systems has started to close the gap between policy and practice in risk management, despite macroeconomic challenges.

In Sub-Saharan Africa, risk management remains underdeveloped but is steadily improving. Financial institutions in Kenya, Nigeria, and South Africa have made strides in credit risk evaluation and digital fraud detection. According to a 2018 study, banks that adopted ERM in Sub-Saharan Africa exhibited a 7–10% increase in profitability due to better credit risk screening and loan loss provisioning (Okpara, 2018). The implementation of Basel II and III has been inconsistent, often due to infrastructural and regulatory limitations. However, technology-driven risk tools, such as mobile-based risk scoring in Kenya, have enhanced outreach while minimizing non-performing loans (NPLs). Local institutions still face hurdles like political risk, currency volatility, and limited regulatory capacity, but targeted reforms are gradually improving the risk management environment.

Cross-comparison of the effectiveness of risk management in financial institutions globally shows that institutional maturity, governance culture, and regulatory oversight are the most significant determinants of success. In high-income countries like the USA and the UK, regulatory sophistication and technological capacity lead to advanced forms of risk modeling and mitigation. By contrast, emerging markets like Brazil and Nigeria emphasize basic risk control and financial education as tools for risk minimization. A global survey published in 2021 found that 73% of financial institutions in OECD countries regularly conduct stress testing, compared to just 29% in Sub-Saharan Africa (Chakraborty & Straub, 2021). This disparity underscores the role of institutional capability and infrastructure in effective risk management.

The rise of climate risk and cyber threats has added new layers of complexity to risk management in the financial sector. In the USA, the SEC has proposed climate risk disclosure rules that require banks to assess and report exposure to climate-related risks. In Japan and the UK, regulatory bodies have introduced green stress testing. According to a 2023 analysis, 82% of top financial institutions in developed countries have integrated environmental risk into their ERM frameworks, while less than 35% of institutions in developing economies have done so (Nguyen & Baker, 2023). This points to a growing divergence in the sophistication of risk modeling between regions.

Technology adoption has dramatically influenced the effectiveness of risk management, especially through predictive analytics and machine learning. Banks in the United States and the UK have leveraged AI to detect patterns of fraud, automate credit scoring, and manage portfolio risks. A 2020 study by Deloitte found that institutions using AI-based risk assessment tools reduced fraud-related losses by up to 25% (Deloitte, 2020). In contrast, Sub-Saharan institutions are in the early stages of deploying such tools due to cost and expertise limitations. Nonetheless, FinTech collaboration is helping bridge this gap through cloud-based risk solutions and mobile platforms that reduce operational risk and increase transparency.

The COVID-19 pandemic served as a real-world test of risk management frameworks across countries. Institutions with strong ERM systems rebounded more quickly, particularly those that had business continuity planning embedded in their risk frameworks. In the UK, financial institutions reported a 40% faster return to pre-pandemic lending volumes compared to those in Latin America (Ahmed et al., 2021). The role of digital resilience and remote risk operations played a significant part in this recovery. This divergence illustrated the importance of not just having a risk management policy but ensuring it is integrated with digital infrastructure and crisis management planning.

While financial institutions globally recognize the importance of risk management, effectiveness varies widely based on regulatory robustness, technological adoption, and institutional readiness. Developed nations have leveraged comprehensive frameworks, data analytics, and proactive supervision to institutionalize risk management as a strategic pillar. Meanwhile, emerging economies are catching up, often driven by regulatory reform, financial inclusion agendas, and technological innovation. Continued progress will depend on harmonizing international standards, cross-border cooperation, and investments in digital risk capabilities.

Cyber threats have evolved from isolated incidents of hacking into a highly organized global phenomenon that undermines the financial ecosystem's stability, especially in banks and related financial institutions. Modern threats encompass a broad spectrum, including ransomware attacks, advanced persistent threats (APTs), phishing campaigns, denial of service (DoS) attacks, and zero-day exploits. The financial sector, given its sensitive data and monetary assets, is disproportionately targeted. In 2022, cyberattacks against financial services firms were 300 times more frequent than in other industries, demonstrating the heightened exposure (Anderson & Agarwal, 2020). As financial institutions migrate more services to digital and cloud platforms, their attack surface expands, challenging traditional risk management strategies. Risk mitigation must now go beyond firewalls and antivirus software to include intelligence-led penetration testing, real-time threat detection systems, and predictive analytics. Without this shift, financial institutions will continue to struggle in safeguarding against the sophisticated and rapidly evolving threat landscape.

In the United States, a nation with one of the most digitized financial ecosystems globally, cyber threats have become a national security concern, especially after major breaches like those at Capital One (2019) and Equifax (2017). These incidents prompted regulatory tightening from agencies such as the Federal Reserve, Office of the Comptroller of the Currency (OCC), and the Federal Financial Institutions Examination Council (FFIEC). U.S. financial institutions now operate under frameworks like the NIST Cybersecurity Framework, which emphasizes real-time monitoring, governance, and rapid incident response (Nguyen & Luong, 2021). However, challenges persist. Small and mid-sized banks often lack the technological sophistication and human capital to deploy comprehensive cybersecurity measures. Furthermore, the fragmented nature of the U.S. regulatory landscape occasionally leads to inconsistent oversight. Despite these challenges, the integration of artificial intelligence and machine learning into cyber risk management has enhanced anomaly detection and threat modeling capabilities in large institutions.

The United Kingdom has taken a proactive approach to cyber threats, especially after the 2017 WannaCry ransomware attack, which disrupted multiple sectors. The Bank of England, through the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), mandates stringent stress testing and vulnerability assessments through programs like CBEST. This intelligence-led testing simulates real-world attacks to gauge institutional resilience (Howard et al., 2020). Moreover, UK financial entities are required to meet the operational resilience expectations set by the PRA, including predefined tolerance levels for service disruption. Although these frameworks are robust, actual implementation across institutions varies, particularly in non-systemically important banks. A recurring challenge is translating threat intelligence into practical, scalable, and responsive defense mechanisms, especially when third-party service providers are involved. Nonetheless, the UK remains a global leader in embedding cyber threat management into the broader enterprise risk landscape.

Japan's financial sector operates with a high degree of technological integration, yet cultural and bureaucratic barriers hinder its full cybersecurity potential. The Financial Services Agency (FSA) of Japan has emphasized cyber resilience in its supervisory guidelines, especially after attacks on major banks like Mitsubishi UFJ and Japan Post Bank (Takahashi & Okubo, 2022). The risk management approach in Japanese banks emphasizes compliance and technical upgrades, such as AI-driven intrusion detection systems. However, challenges persist in fostering real-time inter-departmental coordination and quick response protocols, due in part to Japan's traditionally hierarchical organizational culture. Cyber incident reporting remains conservative, and lessons from cyber events are not always translated into dynamic policy shifts. While the country is investing in quantum-resistant cryptography and blockchain security, the effectiveness of risk management still depends on overcoming internal silos and bureaucratic inertia.

Brazil's banking system is experiencing one of the fastest digital transformations in the world, led by open banking initiatives and fintech growth. However, this rapid digitization has exposed the country's financial institutions to cyber vulnerabilities. According to Resolution 4,658 by the Central Bank of Brazil, institutions must now develop contingency plans, ensure data confidentiality, and establish cyber governance structures (Santos & Figueiredo, 2020). Yet compliance and implementation vary widely. While large banks have invested heavily in AI-driven security tools, smaller institutions struggle due to financial and technological constraints. Incidents of ransomware and phishing have risen sharply—reportedly a 200% increase in attacks against fintechs between 2019 and 2022. Without a national cyber threat intelligence hub and more stringent enforcement, Brazil's risk management strategies remain reactive rather than proactive.

Sub-Saharan African financial institutions are increasingly exposed to cyber threats as mobile banking and digital payment systems expand rapidly. In countries like Nigeria and Kenya, mobile money transactions now account for more than 60% of financial flows, making them prime targets for malware and SIM swap attacks (Munyua & Musau, 2021). Unfortunately, risk management systems in this region often lack real-time detection capabilities and are rarely integrated with global threat intelligence platforms. Many financial institutions operate on legacy infrastructure, with minimal investment in staff training or cyber resilience. Furthermore, national cybersecurity policies are either nascent or unenforced. While some regional efforts, such as Nigeria's Cybercrime Act and Ghana's Cybersecurity Authority, show promise, their influence is limited by cross-border jurisdictional issues and lack of regional coordination.

An institution's ability to transform cyber threat data into actionable intelligence significantly determines its risk management effectiveness. In the USA and UK, advanced cyber threat intelligence (CTI) systems are increasingly embedded within enterprise risk management frameworks. These systems use machine learning to detect anomalies, forecast threat trends, and prioritize responses. Conversely, Japanese and Brazilian institutions often underutilize threat intelligence due to integration gaps or limited cross-agency cooperation (Cheng, Fu & Wu, 2019). Sub-Saharan African banks lag even further behind, with few having access to real-time global threat feeds. The difference in CTI deployment creates a disparity in incident response times and recovery effectiveness, ultimately influencing the sector's stability. Collaborative efforts like FS-ISAC aim to reduce this gap, but participation is skewed toward institutions from developed nations.

Effective cyber risk management requires board-level engagement. Boards that understand cyber risk as a strategic, not merely technical, issue tend to implement more resilient systems. In countries like the UK and USA, regulators have begun to hold boards accountable for cyber incidents. The Bank of England's "Dear CEO" letters emphasize the responsibility of senior management in ensuring cyber resilience (Allen, Gu & Kowalewski, 2020). In contrast, Brazilian and African boards often delegate cybersecurity oversight to IT departments, resulting in fragmented responses and misaligned priorities. Japanese institutions are gradually increasing board literacy through mandatory cyber risk education programs, though cultural resistance persists. Globally, aligning cyber risk with enterprise risk and business continuity strategies remains a critical frontier.

Cyber threats are no longer isolated technical glitches—they are systemic risks capable of destabilizing national and global financial systems. For instance, a successful attack on a national payment system or interbank settlement platform could lead to liquidity shortages and public panic, triggering systemic collapse. Japan's Zengin system, the US Fedwire, and UK's CHAPS all exemplify critical financial infrastructure vulnerable to cyber disruptions (Gyamfi & Boateng, 2022). Most institutions lack contingency plans for prolonged outages or cascading failures. Risk management strategies must therefore extend beyond organizational silos and incorporate macroprudential cyber risk assessments and coordinated sector-wide incident simulations.

The future of effective cyber risk management lies in leveraging AI for predictive analytics, automating response protocols, and building global coalitions for threat mitigation. Emerging threats from deepfake fraud, quantum computing, and synthetic identity creation necessitate advanced preparedness. Countries like the US and UK are investing in next-gen solutions, while Brazil and Sub-Saharan Africa require international support for capability building. Initiatives like the EU–Africa Cyber Resilience Partnership and FS-ISAC promote shared defense, but their long-term success depends on inclusive participation, data democratization, and technical harmonization (Nguyen & Luong, 2021). Financial institutions must now think globally but act institutionally, embracing integrated frameworks that embed cyber resilience as a core business objective.

1.1 Statement of the Problem

Strategic risk management in the financial sector is increasingly being redefined by the scale, sophistication, and frequency of cyber threats. The financial services industry, which once concentrated strategic risk initiatives on credit, liquidity, and operational exposures, now faces growing challenges posed by cyberattacks that can destabilize entire markets. Recent reports show that cybercrime cost the global financial sector over $6 trillion in 2021 alone, with banks experiencing a 238% surge in cyberattacks during the COVID-19 pandemic (Accenture, 2021). This alarming trend has elevated cybersecurity from a technical issue to a strategic board-level concern. Despite this, many financial institutions still adopt reactive, siloed approaches to cyber threats, leading to fragmented strategic responses. Consequently, there is a pressing need to explore how financial institutions embed cyber resilience into their strategic risk management frameworks and whether such integration translates into actionable governance and adaptive strategies.

Previous literature tends to address cybersecurity from either a technical or compliance perspective, focusing heavily on IT departments, threat detection, and regulatory alignment. However, limited research has empirically examined how cybersecurity concerns are strategically framed, prioritized, and managed across leadership, governance, and enterprise-level planning in financial institutions. In particular, studies rarely link cyber risks with dynamic strategy, enterprise transformation, or value creation. This leaves a research gap regarding how cyber threats are institutionally internalized and strategically managed in different regulatory, market, and organizational contexts. Hence, the current study aims to fill this void by investigating how strategic risk management is evolving in response to cyber threats, and what frameworks, capabilities, or institutional pressures facilitate or inhibit this evolution (Zhang, Ponomareva & Lupu, 2019).

The findings of this study will benefit a variety of stakeholders. First, senior executives and board members in financial institutions can leverage the insights to enhance decision-making and governance practices around cyber resilience. Second, regulators and policymakers may utilize the findings to design more effective, risk-based compliance frameworks tailored to real-world strategic needs rather than mere checklist conformity. Third, academics and researchers will benefit from a multidimensional understanding of how financial institutions respond strategically to cyber threats, contributing to the refinement of ERM and institutional theory in digital environments. Lastly, customers and investors stand to gain from the improved stability and trust that result when financial institutions develop robust strategic responses to evolving cyber threats (Eling & Schnell, 2016).

2.0 LITERATURE REVIEW

2.1 Theoretical Review

2.1.1 Enterprise Risk Management (ERM) Theory

Originating from organizational and financial management disciplines, the Enterprise Risk Management (ERM) theory was formalized through frameworks developed by bodies such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and refined in scholarly literature by authors like Lam (2003). ERM posits that organizations can attain strategic goals by identifying, assessing, and managing risks holistically across departments and levels. The key premise is that risk is not merely a threat but a component of value creation when strategically managed. In the context of cyber threats affecting financial institutions, ERM offers a robust lens to investigate how strategic risk management frameworks are adapting to incorporate digital vulnerabilities into enterprise-wide risk assessments. Financial institutions are under increasing pressure to evaluate cyber threats not just from an operational or IT perspective but from a strategic, cross-functional vantage. As ERM emphasizes integrated governance and strategic alignment of risk practices, it provides a comprehensive foundation to explore how banks and financial organizations are modifying their internal controls, board governance, and investment priorities to manage evolving cyber risks. This theory is essential to uncover whether current frameworks in financial institutions align with global standards in the face of cyber disruptions (Lam, 2003).

2.1.2 Dynamic Capabilities Theory

The Dynamic Capabilities Theory, developed by Teece, Pisano, and Shuen in 1997, emphasizes an organization's ability to integrate, build, and reconfigure internal and external competencies in response to rapidly changing environments. In the era of cyber threats, where adversaries constantly evolve in sophistication, financial institutions must not only respond to current risks but also develop the capacity to anticipate and adapt to new threat landscapes. Dynamic capabilities are particularly relevant to strategic risk management as they highlight agility, innovation, and learning as pillars of sustained competitive advantage. Applied to cyber risk, this theory helps explain how institutions that continuously update their cybersecurity protocols, employee training programs, and technology stacks are better positioned to handle sophisticated cyberattacks. This perspective also supports investigations into how institutional leadership and culture foster or hinder the evolution of risk frameworks under digital duress. The theory thus illuminates whether financial institutions are evolving in step with cyber challenges or falling behind due to inertia or structural rigidities (Teece, Pisano and Shuen, 1997).

2.1.3 Institutional Theory

Institutional Theory, championed by scholars like DiMaggio and Powell (1983), explains how organizations conform to prevailing norms, regulations, and cultural expectations to gain legitimacy and ensure survival. This theory underscores the role of external pressures—such as regulatory bodies, professional associations, and public scrutiny—in shaping organizational behavior. In relation to strategic risk management and cyber threats, Institutional Theory is vital for understanding how financial institutions react to global cybersecurity mandates, compliance expectations like GDPR or PCI-DSS, and stakeholder pressure to enhance cyber resilience. The theory reveals why firms often mimic the cybersecurity strategies of peers (mimetic isomorphism), comply with laws even if they are reactive (coercive isomorphism), or adopt standards to appear legitimate to investors and clients (normative isomorphism). In strategic terms, it helps assess whether the implementation of cybersecurity policies in financial institutions is truly driven by risk-based assessments or by the need to conform to institutional pressures, thereby potentially creating gaps in proactive risk posture (DiMaggio & Powell, 1983).

2.2 Empirical Review

Eling & Schnell (2016) examined how insurers integrate cyber risks into their Enterprise Risk Management (ERM) frameworks, with a particular focus on leading financial institutions in Europe. The study used a qualitative case study methodology, analyzing a range of data sources, including detailed reports and in-depth interviews with key stakeholders within these institutions. The findings revealed that while firms acknowledge the importance of cyber risk as a critical concern, their integration into strategic risk planning remained superficial. Many institutions lacked advanced monitoring capabilities for real-time cyber threats, and often, cyber risks were narrowly treated as an IT issue, rather than a strategic risk that could impact broader business operations. The authors suggested that firms should embed cyber threats within scenario planning and elevate discussions about these risks to the board level, encouraging a more proactive and comprehensive approach to cybersecurity.

Bouveret (2018) utilized a quantitative econometric approach to analyze the financial impacts of cyberattacks on financial firms, using data from the Bank for International Settlements (BIS) and the International Monetary Fund (IMF). The study highlighted that cyber incidents typically led to significant stock price drops, with an average decline of around 5%, and that the cumulative financial losses were substantially higher for firms that lacked dedicated cyber risk teams. The study underscored the lack of strategic planning surrounding cyber resilience within many financial institutions and stressed the need for stronger governance and risk management frameworks to address these emerging threats. In particular, Bouveret called for cross-border coordination and the establishment of strategic cyber risk reserves to mitigate the financial impacts of such attacks and ensure greater industry-wide resilience.

Kopp, Kaffenberger & Wilson (2017) used network theory to investigate the propagation of systemic risk within financial systems as a result of cyber incidents. Their study, which involved simulating cyberattacks on interconnected financial networks, revealed that if cyber risks were not managed at the strategic enterprise level, the likelihood of cascading failures within the financial system was high. The study demonstrated the interconnected nature of the financial markets and how a single cyber incident could potentially trigger widespread disruptions. These findings emphasized the need for ERM-based cybersecurity strategies that incorporate network theory into the risk management process to enhance the resilience of financial institutions.

Zhang, Ponomareva & Lupu (2019) conducted surveys across various U.S. banks to assess the level of cybersecurity governance maturity and alignment with overall risk strategy. Using logistic regression analysis, the study found that only 35% of banks had developed a cybersecurity strategy that was well-integrated into their broader risk management frameworks. This disconnect between cybersecurity governance and strategic risk management was highlighted as a major vulnerability, especially in light of increasing cyber threats. The authors recommended embedding cybersecurity governance into board-level risk committees to ensure that cyber risks were managed in tandem with other strategic business risks.

Sahin & Duman (2020) investigated the strategic responses of Turkish financial institutions to cyber threats, employing the Delphi method to collect expert opinions. The study found that, despite a high level of awareness regarding the growing cyber threats, many financial institutions were not strategically prepared to handle such risks. One key finding was the significant gap in employee awareness programs and cyber risk simulation exercises. The study highlighted that strategic investment in simulation training and enhancing employee readiness could better equip institutions to mitigate cyber threats. The authors recommended a more proactive, strategic approach to cybersecurity risk management in Turkish financial institutions to bridge the existing preparedness gap.

Ahmed, Mensah & Owusu (2021) conducted a multi-case study analyzing the strategic responses of five African banks to cyber threats. The study found that, similar to other regions, many African financial institutions had a limited strategic approach to managing cyber risks, with cybersecurity often treated as a compliance issue rather than a critical component of enterprise strategy. Furthermore, there was little involvement from the board of directors in cybersecurity decision-making, and many institutions lacked a comprehensive strategy to address evolving cyber threats. The study recommended integrating cyber risks into strategic scorecards and aligning leadership Key Performance Indicators (KPIs) with cybersecurity objectives to ensure that these risks were treated with the same level of importance as other strategic risks.

Peterson & Park (2022) explored the influence of cybersecurity threats on enterprise strategy, focusing on U.S. credit unions. Using structured interviews and document analysis, the study found that institutions that actively engaged in real-time threat intelligence were better able to adapt their strategies in response to emerging cybersecurity risks. The findings indicated that strategic agility, supported by a strong cybersecurity foresight framework, allowed these institutions to better handle cyber disruptions and maintain operational continuity. The authors recommended that financial institutions invest in dynamic strategic planning, ensuring that cybersecurity considerations were integrated into the organization’s long-term strategic objectives.

3.0 METHODOLOGY

The study adopted a desktop research methodology. Desk research refers to secondary data or that which can be collected without fieldwork. Desk research is basically involved in collecting data from existing resources hence it is often considered a low cost technique as compared to field research, as the main cost is involved in executive’s time, telephone charges and directories. Thus, the study relied on already published studies, reports and statistics. This secondary data was easily accessed through the online journals and library.

4.0 FINDINGS

This study presented both a contextual and methodological gap. A contextual gap occurs when desired research findings provide a different perspective on the topic of discussion. For instance, Peterson and Park (2022) explored the influence of cybersecurity threats on enterprise strategy, focusing on U.S. credit unions. Using structured interviews and document analysis, the study found that institutions that actively engaged in real-time threat intelligence were better able to adapt their strategies in response to emerging cybersecurity risks. Their study emphasizes the importance of real-time threat intelligence and how institutions can adapt their strategies dynamically in response to cybersecurity threats, underlining the role of strategic agility and long-term planning in financial institutions. This study goes beyond mere risk management and delves into how institutions can proactively anticipate and adapt to cybersecurity threats for operational continuity. On the other hand, the current study focused on investigating strategic risk management in the age of cyber threats.

Secondly, a methodological gap also presents itself, for example, in exploring the influence of cybersecurity threats on enterprise strategy, focusing on U.S. credit unions- Peterson and Park (2022) used structured interviews and document analysis, and the study found that institutions that actively engaged in real-time threat intelligence were better able to adapt their strategies in response to emerging cybersecurity risks. Whereas, the current study adopted a desktop research method.

5.0 CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The study concluded that financial institutions had fallen short in addressing the emerging threat of cyber risks within their broader strategic risk management frameworks. Despite increasing awareness of cyber threats, many institutions continued to treat cybersecurity as a technical issue rather than an integral component of their overall risk strategy. This limited perspective resulted in reactive rather than proactive responses to cyber risks, which heightened the vulnerability of these institutions to cyberattacks. The research found that, while certain financial organizations recognized the financial and operational impact of cyber threats, many lacked the necessary strategies to manage these risks effectively at the enterprise level.

It became clear that traditional risk management frameworks were insufficient to handle the rapidly evolving nature of cyber threats. Financial institutions that failed to integrate cybersecurity into their strategic planning were found to be less resilient and more susceptible to large-scale cyber incidents. The study also identified a significant disconnect between the leadership of financial institutions and their cybersecurity teams, with boards of directors often not fully engaged in cybersecurity governance. This lack of involvement at the top levels of management further contributed to poor decision-making when addressing cybersecurity risks.

Moreover, the study highlighted that many financial institutions had yet to adopt a comprehensive enterprise-wide approach to cybersecurity. Rather than viewing cyber threats as a systemic risk that could impact the stability of the financial system as a whole, these institutions often relegated cybersecurity to isolated IT departments. As a result, there was a lack of coordination across departments and inadequate resources allocated to address cybersecurity challenges. This failure to incorporate cyber risk into enterprise risk management (ERM) frameworks left financial institutions ill-prepared to respond to cyberattacks effectively.

The study argued that financial institutions needed to fundamentally rethink their approach to risk management in the age of cyber threats. Effective management of cyber risks required a strategic shift toward integrating cybersecurity into the core of decision-making at all levels of the organization. It was crucial for institutions to develop more robust, forward-looking strategies to address the evolving threat landscape, ensuring that cybersecurity became a central aspect of their risk management frameworks and overall strategic planning.

5.2 Recommendations

The study made several recommendations for improving strategic risk management in financial institutions, particularly in the context of cybersecurity. It emphasized the importance of integrating cybersecurity into the broader enterprise risk management framework. This integration would ensure that cyber risks were considered in the same light as other critical risks, such as market, credit, and operational risks. Financial institutions were encouraged to involve their boards of directors in cybersecurity governance, making cybersecurity a priority at the highest levels of decision-making. This would ensure that cybersecurity received the attention and resources it needed to be managed effectively.

Another key recommendation was the need for financial institutions to adopt a proactive approach to cybersecurity. The study called for a shift away from reactive measures and emphasized the importance of anticipating potential cyber threats before they could materialize into full-blown incidents. Institutions were advised to invest in real-time threat intelligence systems and to establish cyber risk monitoring capabilities that could provide up-to-date insights into the evolving threat landscape. By adopting such measures, financial institutions could respond more quickly and effectively to emerging threats, minimizing their impact on operations and financial stability.

In addition to technological improvements, the study recommended that financial institutions invest in the development of internal expertise. This included enhancing the skills of cybersecurity teams and providing ongoing training for employees to raise awareness about cyber threats. Moreover, it was suggested that institutions build cross-departmental collaboration to ensure that cybersecurity was not siloed in the IT department but was treated as a strategic risk across all business units. This approach would help break down organizational silos and foster a more comprehensive and coordinated response to cyber risks.

From a policy perspective, the study recommended that regulators and policymakers play a more active role in guiding financial institutions toward better cybersecurity practices. The establishment of clear and consistent cybersecurity standards was seen as critical to improving the sector's resilience. The study suggested that governments should implement policies that encourage financial institutions to adopt cybersecurity frameworks that are aligned with international best practices. Additionally, it recommended that regulators promote the development of public-private partnerships to share knowledge and resources, which would enhance the overall cybersecurity posture of the financial sector.

In terms of contributions to theory, the study advanced the concept of integrating cybersecurity into strategic risk management. It introduced the idea of cybersecurity as a systemic risk that needed to be managed in conjunction with other strategic risks. The research contributed to the growing body of literature on cyber risk governance by proposing that financial institutions needed to view cybersecurity through a broader lens, considering its potential to impact the stability of financial systems. By advocating for the strategic inclusion of cybersecurity within risk management frameworks, the study helped bridge the gap between traditional risk management practices and the emerging realities of the digital age.

Finally, the study's contributions to practice were significant, particularly in terms of its actionable recommendations for financial institutions. The practical implications of the study offered clear guidance on how financial institutions could enhance their cybersecurity governance, from strategic planning to employee training and cross-departmental collaboration. The findings emphasized the need for continuous investment in cybersecurity resources and the importance of real-time monitoring. As financial institutions grapple with an increasingly complex and interconnected cyber threat landscape, the study provided a roadmap for institutions to navigate these challenges and build more resilient cybersecurity infrastructures.

REFERENCES

Accenture. (2021). The cost of cybercrime: A rise in financial sector attacks. https://www.accenture.com/us-en/insights/security/cost-cybercrime

Ahmed, A., Mensah, A., & Owusu, E. (2021). Cyber risk governance in emerging markets: A case of African financial institutions. Information & Computer Security, 29(3), 455–472. https://doi.org/10.1108/ICS-03-2021-0032

Ahmed, K., Rana, R., & Muzaffar, M. (2021). Business continuity and financial risk mitigation during COVID-19. Global Finance Journal, 51, 100626. https://doi.org/10.1016/j.gfj.2021.100626

Allen, F., Gu, X., & Kowalewski, O. (2020). Cybersecurity and financial stability: Evidence from the banking industry. Journal of Financial Stability, 47, 100705. https://doi.org/10.1016/j.jfs.2019.100705

Anderson, R., & Agarwal, A. (2020). Cybersecurity risk in banking systems: A case analysis of Equifax. International Journal of Finance & Banking Studies, 9(1), 65–78. https://doi.org/10.20525/ijfbs.v9i1.1022

Baker, H., & Frame, S. (2022). Financial innovation, regulatory response, and risk management: Evidence from the UK. International Review of Financial Analysis, 82, 102171. https://doi.org/10.1016/j.irfa.2022.102171

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper. https://www.imf.org/en/Publications/WP/Issues/2018/07/13/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-46076

Chakraborty, I., & Straub, D. (2021). Institutional capacity and the global effectiveness of financial risk management. Journal of Financial Stability, 53, 100849. https://doi.org/10.1016/j.jfs.2021.100849

Cheng, C., Fu, X., & Wu, L. (2019). Cyber threat intelligence integration: A comparative study of US and Japanese banks. Cybersecurity, 3(1), 12. https://doi.org/10.1186/s42400-019-0032-1

Deloitte. (2020). AI and the Future of Risk Management. Deloitte Insights. https://doi.org/10.2139/ssrn.3564047

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? Journal of Risk Finance, 17(5), 474-491. https://doi.org/10.1108/JRF-09-2016-0013

Gonçalves, T. F., Silva, A. L., & Matos, L. C. (2020). Financial regulation, risk, and performance: Evidence from Brazil. Emerging Markets Review, 45, 100717. https://doi.org/10.1016/j.ememar.2020.100717

Gyamfi, M., & Boateng, E. (2022). Cybersecurity vulnerabilities and the banking sector in Sub-Saharan Africa. African Journal of Information Systems, 14(2), 33–49. https://digitalscholarship.unlv.edu/ajis/vol14/iss2/2

Howard, S., Miller, D., & Behrens, T. (2020). Cyber risk stress testing in the UK banking sector: The CBEST framework. Journal of Financial Regulation and Compliance, 28(3), 410–426. https://doi.org/10.1108/JFRC-02-2020-0018

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. IMF Working Paper. https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45105

Lam, J. (2003). Enterprise Risk Management: From Incentives to Controls. Wiley.

Lundqvist, S. A. (2021). Enterprise risk management and firm performance: The role of firm size and risk management culture. Journal of Risk and Financial Management, 14(2), 89. https://doi.org/10.3390/jrfm14020089

Munyua, L., & Musau, J. (2021). The state of cybersecurity risk management in Sub-Saharan Africa’s financial institutions. Information & Computer Security, 29(4), 545–560. https://doi.org/10.1108/ICS-10-2020-0156

Nguyen, T. H., & Baker, R. J. (2023). Climate risk and enterprise resilience in the financial services industry. Journal of Sustainable Finance & Investment. https://doi.org/10.1080/20430795.2023.2172654

Nguyen, T., & Luong, T. (2021). Evaluating cybersecurity frameworks for financial institutions: A U.S. perspective. Journal of Cybersecurity Research, 6(1), 45–59. https://doi.org/10.1145/3453873

Okpara, G. C. (2018). Enterprise risk management and performance of financial institutions in Sub-Saharan Africa. African Journal of Economic Policy, 25(2), 45–67. https://doi.org/10.4314/ajep.v25i2.4

Peterson, R., & Park, S. (2022). Cybersecurity foresight and strategic agility in financial institutions. Journal of Strategic Security, 15(1), 92–118. https://doi.org/10.5038/1944-0472.15.1.1945

Sahin, H., & Duman, H. (2020). Strategic cyber risk management in Turkish banking sector. Procedia Computer Science, 176, 1054–1063. https://doi.org/10.1016/j.procs.2020.09.143

Saito, Y., Takahashi, T., & Kimura, H. (2019). Risk governance and performance: Evidence from Japanese banks. Journal of Banking & Finance, 106, 423–437. https://doi.org/10.1016/j.jbankfin.2019.07.004

Santos, D., & Figueiredo, L. (2020). The challenge of cybersecurity in Brazilian digital banking. Brazilian Journal of Information Systems, 13(2), 76–91. https://doi.org/10.1590/s1234-2020-1345

Takahashi, K., & Okubo, Y. (2022). Risk governance and cyber resilience in Japanese financial institutions. Journal of Asian Economics, 80, 101482. https://doi.org/10.1016/j.asieco.2022.101482

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Managemen

World Bank. (2023). Global Financial Development Report: Financial Resilience in a Changing World. https://doi.org/10.1596/978-1-4648-1897-5

Zhang, J., Ponomareva, Y., & Lupu, I. (2019). Strategic alignment of cybersecurity governance in financial services. Computers & Security, 87, 101568. https://doi.org/10.1016/j.cose.2019.101568