DELSU Journal of Management Sciences
Abbr. Title: Deljoms, FMS
ISSN: *(Online)* **: 2756-3731**
OPEN ACCESS
Research Article Volume 7 Number 1 June, 2025

Cybersecurity and Firm Performance: Bridging the Gap between Protection and Profitability

Monye-Emina, Henry Emife[1] and Origho Victor Fegor[2]
[1]Department of Accounting,
University of Benin, Benin-City, Edo State, Nigeria.
henry.monye-emina@uniben.edu

[2]Department of Accounting,
Dennis Osadebey University,
Asaba, Delta State, Nigeria.
origho.victor@dou.edu.ng

Publication Date: 2025/06/30

Abstract
In an increasingly digital economy, cybersecurity has transitioned from a mere information technology concern to a critical component of organisational strategy. This paper conceptually explores the relationship between cybersecurity practices and firm performance. It argues that robust cybersecurity strategies not only mitigate risks but also contribute positively to business outcomes, enhancing consumer confidence, ensuring operational continuity, and promoting competitive advantage. Key themes discussed include the concept of cybersecurity, Cybersecurity as a driver of strategic advantage, Governance and regulatory impacts, we also consider the various cybersecurity framework and lastly conclusion and recommendations. This paper aims to help practitioners and scholars understand the multifaceted impact of cybersecurity on organisational efficacy.

Keywords: *Cybersecurity, Governance, vulnerabilities, strategic advantage, operational viability.*

Introduction

The digital transformation of businesses has unlocked new opportunities for growth and efficiency, but it has also ushered in a wave of cyber threats that pose significant risks to organisations. High-profile security breaches have demonstrated the vulnerabilities underlying even the most seemingly secure infrastructures, leading to increased scrutiny from stakeholders regarding firms' cybersecurity measures. As organisations grapple with these challenges, the question arises: how does cybersecurity influence firm performance.

In today's hyper-connected world, businesses face unprecedented opportunities and challenges stemming from rapid technological advancements. The proliferation of digital platforms, cloud computing has revolutionized how organisations operate, providing avenues for innovation, efficiency, and customer engagement. However, this digital transformation has also exposed firms to a complex and evolving landscape of cyber threats (Saeed, et al., 2023). High-profile data breaches, ransomware attacks, and other malicious cyber activities have become alarmingly commonplace, with statistics indicating that cybercrime costs the global economy trillions of dollars annually (Gordon, et al., (2018). Against this backdrop, the imperative for effective cybersecurity practices has never been more pressing. Stakeholders, including customers, investors, regulators, and employees, are increasingly aware of the potential repercussions of inadequate cybersecurity measures. Acknowledging this reality, firms must navigate a dual challenge: addressing the barrage of cyber threats while simultaneously leveraging cybersecurity as a strategic asset that can enhance overall performance.

This study posits that cybersecurity is not just a shield against potential threats but also a catalyst for firm performance. By examining the nuanced interplay between cybersecurity practices and organisational success, we aim to provide a comprehensive framework that elucidates how sound cybersecurity investments can yield significant returns. Evidence suggests that firms prioritizing cybersecurity can foster greater customer trust, ensure uninterrupted service delivery, and differentiate themselves in competitive markets. Moreover, as regulatory scrutiny intensifies, compliance with cybersecurity standards becomes increasingly intertwined with firm reputation and operational viability (Saeed, et al., 2023).

Literature Review

Concept of Cybersecurity in Organisations

The defence of internet-connected devices and services against malevolent attacks by hackers, spammers, and cybercriminals is known as cybersecurity. This approach is used by businesses to guard against identity theft, ransomware attacks, phishing tactics, data breaches, and financial losses. Cybersecurity also refers to any technologies, practices and policies for preventing cyberattacks or mitigating their impact (Lopatova, 2021). The goal of cybersecurity is to defend against ransomware, other malware, phishing scams, data theft, and other cyberthreats by safeguarding computer systems, apps, devices, data, financial assets, and individuals. Cybersecurity is a crucial part of an organization's entire risk management plan at the corporate level. Cybersecurity Ventures predicts that between 2021 and 2025, global spending on cybersecurity goods and services would surpass USD 1.75 trillion. Job growth in cybersecurity is also strong. The US Bureau of Labor Statistics projects that "employment of information security analysts is projected to grow 32% from 2022 to 2032, faster than the average for all occupations (Saeed, et al., 2023). Because cyberattacks and cybercrime have the potential to disrupt, harm, or even destroy communities, businesses, and

individuals, cybersecurity is crucial. Successful cyberattacks lead to identity theft, personal and corporate extortion, loss of sensitive information and business-critical data, temporary business outages, lost business and lost customers and, in some cases, business closures (Berry, et at., 2018). Cyberattacks have an enormous and growing impact on businesses and the economy. By one estimate, cybercrime will cost the world economy USD 10.5 trillion per year by 2025. The cost of cyberattacks continues to rise as cybercriminals become more sophisticated.

Cybersecurity as a Driver of Strategic Advantage

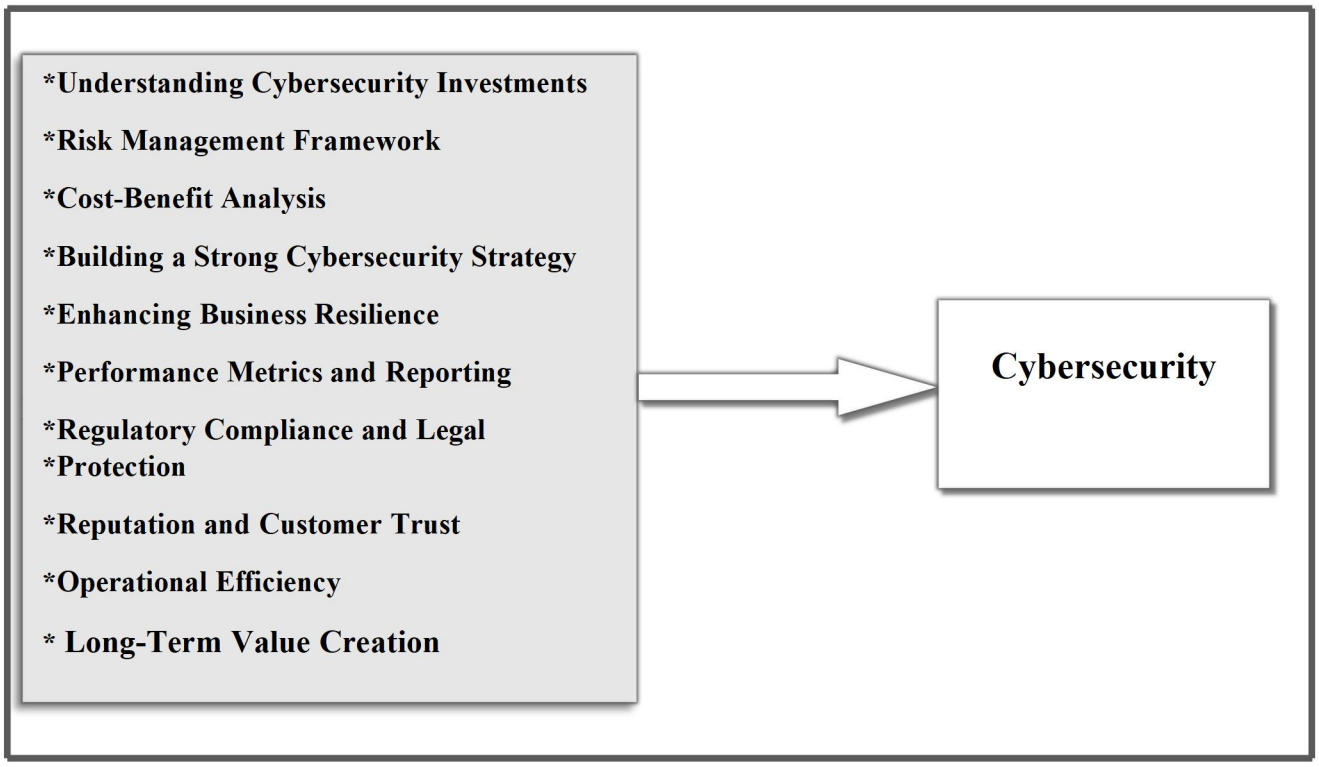
Cyber security is now a key differentiator in a world that is becoming more interconnected; it is no longer merely a question of risk management. To succeed in the market, information security must be utilized as a strategic instrument. The majority of leaders consider cybersecurity to be a means of thwarting threats. But in today's intensely competitive digital economy they should be thinking about cybersecurity as a strategic advantage that not only protects business value, but enables new business value (Castillo, et al., 2018). It is not unexpected that dangers are the main emphasis in order to preserve company value. In today's ever-changing threat landscape, modern digital firms transcend conventional boundaries and give rise to new attack vectors. Companies are dealing with a surge of cybercrime that is getting more sophisticated and intense. According to a recent article in Forbes, "Corporate and home computers have been hit with an average of 4,000 ransomware attacks every day this year, a 300% increase over 2015," citing United States Department of Justice sources (Saeed, et al., 2023). The greatest chance for growth will arise when we make cybersecurity a key element of our digital plans, even while we still need to work hard to safeguard important data and assets. The fact that cybersecurity flaws stifle innovation is one of its main drawbacks. Indeed, according to a Cisco poll, 71% of participants stated that cybersecurity threats and risks impede organizational innovation. Organisations that have any doubt about their cybersecurity capabilities delay important digital initiatives and risk falling behind competitors (Saeed, et al., 2023).

Governance and Regulatory Impacts

Safeguarding sensitive data within your organization and preserving stakeholder trust depend on effective cyber security governance. Legal liabilities, financial losses, and harm to one's reputation can all arise from poor governance. Lebogang, Tabona, and Maupong (2022) evaluated national cybersecurity strategies across Africa, highlighting Nigeria's initiatives as part of a broader continental effort to secure cyberspace. In line with this, Ikuero (2022) detailed the Nigerian government's establishment of a national Computer Emergency Response Team (CERT), Sectoral Computer Security Incident Response Teams (CSIRTs), and the formulation of the National Cybersecurity Policy and Strategy (NCPS) through the Office of the National Security Adviser (ONSA), aiming to enhance cybersecurity coordination within the country. Despite these efforts, Nte, Enoke, and Teru (2022) identified weaknesses in Nigeria's cyber laws and policies, noting the national documents, while comprehensive in some areas, failed to address all aspects of cyber security concerns. The banking sector, as a critical component of Nigeria's economy, has adopted key strategies to bolster cybersecurity defences against escalating cyber threats. According to Reis, Oliha, Osasona, and Obi (2024), Nigerian banks are battling threats like ransomware, phishing, and insider assaults by using advanced security technologies, training their employees, and working with international cybersecurity

organizations and the government. Additionally, the digital economy's growth in Nigeria necessitates robust cybersecurity measures due to increased cyber-attack risks (Ukwuoma, Williams, & Choji, 2022). The rise of cybercrime on social media has prompted research into common scams, tactics used by cybercriminals, and recommendations for enhancing cybersecurity awareness and protective measures (Damilolo, Emmanuel, & Ngoc, 2023). Furthermore, the study by Garba, Siraj, and Othman (2022) focused on assessing cybersecurity awareness among university students in Northeastern Nigeria, indicating a need for comprehensive education on various cybersecurity aspects. International perspectives on cybersecurity strategies provide useful insights for Nigeria. Sabillon (2022.) discussed phases in unifying national cybersecurity strategy models, emphasizing the importance of developing international strategies, alliances, and cooperation. Similarly, cybersecurity strategies for SMEs in the Nordic Baltic Region, focusing on awareness, training, and financial incentives (Falch et al., 2023), offer potential lessons for Nigerian enterprises. Cybersecurity in Nigeria faces challenges including legal and policy gaps, threat evolution, and the need for greater awareness and education. Strengthening Nigeria's cybersecurity infrastructure requires a multifaceted approach encompassing policy reform, technological advancements, international cooperation, and comprehensive education and training programs.

Cybersecurity Framework



Investing in cybersecurity is vital for organisations in today's digital landscape. A comprehensive framework that elucidates how sound cybersecurity investments can yield significant returns involves several key components of which understanding cybersecurity investments should be the first step. These may include software solutions

(firewalls, intrusion detection systems), hardware (secure servers), personnel training, compliance programs, and incident response planning. These can be of great benefits to the organisation through prevention of data breaches and associated costs, and can also involve enhanced brand reputation and customer trust.

Risk management framework can be achieved through assess the specific cybersecurity risks to the organisation, including the potential impact of data breaches, financial loss, and reputational damage and organisations are to regularly conduct assessments to evaluate vulnerabilities and potential threats to inform investment decisions. On another hand, cost-benefit analysis should also help to calculate the costs associated with investing in cybersecurity technologies, staff training, and policies and can help reduced likelihood of data breaches, lower recovery costs, and avoidance of regulatory fines.

Organisations are also advised to building a strong cybersecurity strategy to establish clear cybersecurity policies and procedures that align with business objectives and compliance requirements and should focus on high-impact areas, such as data protection, network security, and employee training, to maximize the return on investment. Enhancing business resilience to develop and regularly update an incident response plan to minimize damage during a cyber event, thereby protecting assets and maintaining operations.

Business continuity planning is another key framework of cybersecurity that ensure that business operations can continue or quickly recover after a cybersecurity incident, further supporting operational resilience. Performance metrics and reporting help to gauge the effectiveness of cybersecurity investments (e.g., number of incidents detected, time to respond). Regulatory compliance and legal protection help ensure compliance with laws and regulations, and also avoiding legal penalties. Reputation and Customer Trust here strong cybersecurity measures can enhance consumer confidence, leading to increased customer loyalty, retention, and acquisition. Organisations known for robust cybersecurity practices can differentiate themselves in the marketplace. Operational Efficiency can lead to greater efficiency in operations by automating monitoring and response processes thereby reducing the risk of cyber incidents minimizes disruptions, allowing employees to focus on their core tasks.

The final stage of the framework can lead any organisation to long-term value creation. Consider cybersecurity as a long-term investment in organisational resilience and sustainability, ultimately contributing to growth and profitability. A strong cybersecurity posture allows businesses to innovate and explore new technologies without the fear of exposing sensitive data. A well-structured approach to cybersecurity investment not only protects against risks but also drives significant financial and strategic returns. Organisations can unlock value through improved resilience, enhanced reputation, regulatory compliance, and operational efficiencies, ultimately leading to better overall performance and competitive advantage in the market.

Review of Related Theories

The relationship between cybersecurity and firm performance is increasingly recognized in both academic literature and practical business applications. Theoretical frameworks help to understand how investments in cybersecurity can influence overall firm performance. Here are some key theoretical bases that support this relationship.

Resource-Based View. The RBV posits that firms possess unique resources and capabilities that can provide a competitive advantage. Cybersecurity measures, such as advanced technologies and skilled personnel,

can be viewed as strategic resources. Firms that effectively leverage these resources may not only protect themselves from cyber threats but also enhance their reputation, customer trust, and ultimately their financial performance.

The Resource-Based View (RBV) of the firm plays a significant role in understanding the relationship between cybersecurity and firm performance. According to RBV, firms that possess unique resources and capabilities can achieve a competitive advantage. In the context of cybersecurity, this includes not only technological assets (like firewalls, intrusion detection systems, etc.) but also human resources (such as skilled cybersecurity professionals) and organisational processes related to risk management and incident response (Dornheim, et al., 2023).

Moreso, effective cybersecurity measures can serve as a differentiator in the market. Firms that are perceived as having strong cybersecurity practices may attract more customers and partners, leading to enhanced market positioning and reputation. This competitive edge can positively influence firm performance through increased sales, customer loyalty, and reduced risk of financial loss from cyber incidents. Cybersecurity is essential for safeguarding valuable intangible assets such as customer data, intellectual property, and brand reputation. The ability to protect these assets effectively helps maintain operational continuity and reduces potential costs associated with data breaches and cyber threats (Amar, 2016). Investing in cybersecurity can lead to long-term cost savings by minimizing the risk of cyberattacks, which can be expensive in terms of both direct losses and reputational damage. By proactively managing cybersecurity risks, firms can avoid significant expenditures that would arise from breaches, thus enhancing overall financial performance. Firms that prioritize cybersecurity are often better positioned to innovate and adopt new technologies. By ensuring a secure environment for digital operations, they can explore opportunities in e-commerce, cloud computing, and digital transformation without compromising security, thereby contributing to sustained performance improvements. Resource-Based View emphasizes that effective cybersecurity is not just a defensive measure but a strategic asset that can enhance firm performance by creating competitive advantages, protecting valuable resources, and enabling innovation. Firms that invest in and cultivate strong cybersecurity capabilities are likely to see improvements in their overall performance (Koniagina, et al.,2023).

Theory of Planned behaviour: According to TPB, attitudes, perceived behavioural control, and subjective norms all have an impact on an individual's behaviour. Organisational culture and employee behaviour towards cybersecurity can impact a firm's security posture. A positive attitude towards cybersecurity, reinforced by training and leadership support, can lead to better security practices, reducing vulnerabilities and enhancing firm performance. The A helpful framework for comprehending how attitudes, subjective standards, and perceived behavioural control affect people's intentions and behaviours—including those pertaining to cybersecurity in businesses—is offered by the Theory of Planned behaviour (TPB). Employees and management are more inclined to take proactive steps, such following security procedures or attending training sessions, when they believe cybersecurity is important and advantageous.

A positive attitude can lead to a culture of security awareness, enhancing overall firm performance by reducing vulnerabilities (Koniagina, et al.,2023). The behaviour of colleagues and leadership can significantly impact individuals' actions regarding cybersecurity. If there is a strong cultural

norm that emphasizes the importance of cybersecurity, employees are more likely to comply with security measures.

This collective approach can lead to improved firm performance as a result of reduced risk exposure. Employees' perceptions of their ability to implement cybersecurity measures (perceived behavioural control) can influence their actual behaviour. If employees feel empowered and equipped with the necessary resources and training to manage cybersecurity practices, they are more likely to act in ways that support firm performance, such as reporting incidents, following protocols, or adopting secure practices (Gordon, et al., 2018) According to TPB, intentions are the most immediate predictor of actual behaviour. If employees intend to adopt cybersecurity best practices due to favorable attitudes, supportive norms, and a sense of control, it can lead to better security outcomes, thereby enhancing overall firm performance. Firms that embed cybersecurity into their organisational culture and encourage positive behaviours through training and leadership support will likely see long-term improvements in performance. Enhanced cybersecurity can lead to reduced incidents of data breaches, lower compliance costs, and improved customer trust—all contributing to better financial performance and competitive advantage. Theory of Planned behaviour suggests that fostering positive attitudes towards cybersecurity, establishing supportive norms, and enhancing employees' perceived control can significantly influence intentional behaviours that ultimately affect firm performance (Castillo & Falzon, 2018).

Innovation and Technology Adoption Theories: These theories examine how organisations adopt new technologies and the innovation process. Firms that adopt cutting-edge cybersecurity technologies may not only mitigate risks but also gain operational efficiencies and reduce costs, contributing to improved performance through innovation. According to Amar (2016), the relationship between cybersecurity and firm performance can also be examined through the lens of innovation and technology adoption theories. This theory explores how new technologies, including cybersecurity solutions, spread within organisations. Businesses are frequently better able to safeguard their assets when they successfully use cutting-edge cybersecurity solutions (such firewalls, intrusion detection systems, and encryption). Successful adoption can enhance firm performance by mitigating risks associated with cyber threats and improving overall operational efficiency (Castillo & Falzon, 2018). TAM highlights how crucial perceived utility and ease of use are to the uptake of new technology. If employees find cybersecurity tools user-friendly and useful in their daily activities, they are more likely to adopt them. Higher adoption rates can lead to stronger security measures, which ultimately support better firm performance by reducing the likelihood of security breaches.

Incorporating advanced cybersecurity measures can lead to innovative business models and practices(Brock & Levy, 2013). For instance, firms that offer enhanced security features may differentiate themselves from competitors, thereby attracting more customers and increasing market share, ultimately contributing to better performance. Innovation and technology adoption theories suggest that there is a positive relationship between effective cybersecurity measures and firm performance. By embracing and properly implementing innovative cybersecurity solutions, firms can not only protect their assets but also enhance their overall competitiveness and operational efficiency in the market. The interplay between cybersecurity and firm performance is multifaceted and can be understood through various theoretical lenses. As businesses increasingly operate within digital

environments, recognizing the importance of cybersecurity investments not only helps in risk mitigation but also supports overall strategic objectives and enhances competitive advantage (Brock & Levy, 2013). In summary, effective cybersecurity practices contribute positively to firm performance by protecting assets, fostering stakeholder trust, and enabling innovation.

Conclusion and Recommendations

According to the study's findings, Nigeria has acknowledged the significance of cybersecurity since enacting the Cybersecurity Act 2015 in response to the recent rise in cybercrimes in the nation. The work made a theoretical contribution to the academic literature. The study provided data on Nigerian internet and mobile subscribers as well as the nation's digital online activity. It presented informants' scholarly opinions on how cybercrimes affect Nigeria's digital economy and national security. Theoretically, the study was successful in establishing a relationship between the growing empirical data from the field of study and the numerous existing claims regarding cybersecurity and national security issues. In order to avoid cybercrimes in Nigeria, the study also has policy implications for the introduction of specific cybersecurity regulatory ideas. The following is a list of the suggestions: The public should be made aware of the necessity of preventing the online disclosure of security codes and other important information by the government and other organizations in charge of ICT regulations; People should be encouraged to notify the organizations in charge of managing cybersecurity policies about any questionable transactions; To make it easier to identify threats, experts should be hired to teach current employees in the appropriate agencies cybersecurity technicalities; Quarterly workshops and media campaigns should be held to inform the public, businesses, and government organizations on the mechanisms of cybercrime and how to take precautions; In order to discourage future criminal activity, those found guilty of cybercrime should face harsh penalties under the Cybersecurity Act of 2015. To facilitate the identification of suspicious calls and transactions, a databank for mobile phones and internet users should be established. This will allow thieves to be caught as soon as they launch an attack.

References

Alexander, G. (2017), The Flame: Questions and Answers, Kaspersky Labs, Kaspersky Labs. Available from: https://www.securelist.com/34344/the-flame-questions-and- answers-51. Retrieved on 2024 Aug 08.

Amar, S. (2016), Spectre of cyberterrorism: A potential threat to India’s national security. *Indian Journal of Research, 5*(3), 1-16.

Anand, K., Krishnan, P., Devendra, K.P. (2014), Facing the reality of cyber threats in the power sector. Energy Policy, 65, 126-133.

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for Cyber Security threats. *International Journal of Business Continuity and Risk Management, 8*(1), 1-10. https://doi.org/10.1504/IJBCRM.2018.090580

Bose, R., & Luo, X. R. (2014). Investigating security investment impact on firm performance International *Journal of Accounting & Information Management, 22*(3), 19 208.https://doi.org/10.1108/IJAIM-04-2014- 0026

Brock, L., & Levy, Y. (2013). The market value of information system (IS) security for e-banking. *Online Journal of Applied Knowledge Management, 1*(1), 1-17.

Castillo, D., & Falzon, J. (2018). An analysis of the impact of Wannacry cyberattack on cyber security stock returns. *Review of Economics & Finance, 13*(3), 93-100.

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. In Computers in Industry (Vol.114). https://doi.org/10.1016/j.compind.2019.103165

Damilola, O., Emmanuel, A., & Ngoc, P.B. (2023). Cybercrime on social media in Nigeria: trends, scams, vulnerabilities and prevention, https://dx.doi.org/10.22624/aims/cseansmart2023p17

Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. Information & Computer Security. https://dx.doi.org/10.1108/ics-07-2023-0116

Falch, M., Olesen, H., Skouby, K.E., Tadayoni, R., & Williams, I. (2023). Cybersecurity strategies for SMEs in the Nordic Baltic Region. *Journal of Cyber Security and Mobility, 11*(6), 727- 754. https://dx.doi.org/10.13052/jcsm2245-1439.1161

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security*.9(5),125-134. https://doi.org/10.4236/jis.2018.92010

Ikuero, F.E., & Zeng, W. (2022). Improving cybersecurity incidents reporting in Nigeria: micro and small enterprises perspectives. *Nigerian Journal of Technology, 41*(3), 512-520. https://dx.doi.org/10.51594/csitrj.v5i2.761

Koniagina, M., Belotserkovich, D., Vorona-Slivinskaya, L., & Pronkin, N. (2023). Measures to ensure cybersecurity and regulation of the internet of things in the Russian federation: Effectiveness assessment. *Journal of Economic Issues, 57*(1), 257-274. https://dx.doi.org/10.1080/00213624.2023.2170136

Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating cybersecurity strategies in Africa. In Cybersecurity capabilities in developing nations and its impact on global security (1-19). IGI Global. https://dx.doi.org/10.4018/978-1-7998-8693-8.ch001

Lopatova, N. (2021) Cybersecurity as a driver of business growth. *Science and Innovations 3* (217): 38-41. https://doi.org/10.29235/1818-9857-2021-3-38-41

Nte, N.D., Enoke, B.K., & Teru, V.A. (2022). A comparative analysis of cyber security laws and policies in Nigeria and South Africa. Law Research

Review Quarterly, 8(2), 233 258. https://dx.doi.org/10.15294/lrrq.v8i2.56486

Ozsungur, F. (2021) Business Management and Strategy in Cybersecurity for Digital Transformation. Handbook of Research on Advancing Cybersecurity for Digital Transformation144-162. https://doi.org/10.4018/978-1-7998-6975-7.ch008

Reis, O., Oliha, J.S., Osasona, F., & Obi, O.C. (2024). Cybersecurity dynamics in Nigerian banking: trends and strategies review. *Computer Science & IT Research Journal, 5*(2), 336-364. https://dx.doi.org/10.51594/csitrj.v5i2.761

Sabillon, R. (2022). National Cybersecurity Strategies. In Research Anthology on Business Aspects of Cybersecurity (pp. 500-513). IGI Global. https://dx.doi.org/10.4018/978-1-6684-3698-1.ch023

Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E., & Alabbad, D. (2023) Digital Transformation and Cybersecurity Challenges for Businesses Resilience: *Issues and Recommendations. Sensors 23* (15). https://doi.org/10.3390/s23156666

Sandhu, K. (2021) Advancing Cybersecurity for Digital Transformation. Handbook of Research on Advancing Cybersecurity for Digital Transformation1-17. https://doi.org/10.4018/978-1-7998-6975-7.ch001

Reis, O., Oliha, J.S., Osasona, F., & Obi, O.C. (2024). Cybersecurity dynamics in Nigerian banking: trends and strategies review. *Computer Science & IT Research Journal, 5*(2), 336- 364. https://dx.doi.org/10.51594/csitrj.v5i2.761