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

Cybersecurity strategies for protecting big data in business intelligence systems: Implication for operational efficiency and profitability

Joshua Ikenna Egerson [1,*], Mosopefoluwa Williams [2], Aramide Aribigbola [3], Maureen Okafor [4] and Adedeji Olaleye [5]

[1] *Management, University of Derby, Kedleston, England, United Kingdom.*
[2] *John Wesly School of Leadership, Carolina University, United States of America.*
[3] *Business Administration and Management, Anderson University, United States of America.*
[4] *Computer Science, Louisiana State University, Louisiana, United States of America.*
[5] *Professional Accountancy, University of London, United Kingdom.*

World Journal of Advanced Research and Reviews, 2024, 23(02), 916–924

Publication history: Received on 28 June 2024, revised on 07 August 2024, and accepted on 10 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2390

Abstract

Cyberattacks might seriously affect public confidence in the banking sector, stop financial activities, and result in large financial losses. The effect of cybersecurity on operational efficiency and profitability of money deposit banks in Nigeria is examined in this quantitative cross-sectional research. Using an infinite population, Cochran's sampling approach was employed to determine the sample size of 385. Data were gathered from 385 employees of money deposit banks in Lagos State. Using Google Forms, electronic distribution of the surveys produced a high response rate of 97% with 372 completed questionnaires. Data were analysed using SPSS and Structural Equation Model. The study found that cybersecurity significantly predicts operational efficiency and profitability of the money deposit banks in Nigeria. The study recommended that money deposit banks should give constant investment in advanced cybersecurity technologies and knowledge top priority. This entails enhancing detection and reaction strategies to promptly handle fresh cyber threats, thus safeguarding operations and customer data.

Keywords: Cybersecurity; Operational effectiveness; Profitability; Dynamic capabilities theory

1. Introduction

Acting as the basis for financial stability and economic development, financial institutions especially money deposit banks are vital to the economy of a nation like Nigeria (Anoke, Igwebuike, Joyce, Agagbo Ogugua, & Odumuato, 2021). Through loan extension, payment management, and financial service provision to individuals, businesses, and governments, they support capital accumulation, investment, and economic development (Fatoki, 2023). But the rising threat of cyberattacks seriously compromises these companies. Cyberattacks might seriously affect public confidence in the banking sector, stop financial activities, and result in large financial losses (Ojeka, Ben-Caleb, & Ekpe, 2017). Moreover, in a new ransomware statistic 71% of Nigerian companies especially financial institutions experienced cyberattacks in 2021; 44% of these companies paid an average ransom of $3.43 million to safeguard their company and preserve crucial data and by 2025, cybercrime is expected to have a global cost of $10.5 trillion (Ikusika, 2022). Therefore, strong cybersecurity policies are needed to guard against these dangers for Nigeria since the banking sector is essential for creating economic activity and supporting development goals (Victiory, Promise & Mike, 2022). This not only protects the financial resources of the government but also preserves the continuous confidence and dependability of financial institutions, which are very vital for the stability of the national economy and development.

* Corresponding author Egerson Joshua

Cybersecurity encompasses a range of procedures and actions designed to guarantee the defence of individual and corporate data, information, and networks against any potential risks, whether generated from inside or outside (Akintoye, Ogunode, Ajayi, & Joshua, 2022). These threats might encompass data/information abuse, computer hacking, unauthorised access and disclosures, and coordinated assaults via the introduction of malware and related superfluous infections (Ojeka et al., 2017). To Too and Mutuku (2023) cybersecurity is a conglomeration of tactics such as risk management, participation, instruction, best practices, and expertise employed to detect, prevent and protect from cyberattacks. It refers to protection against unlawful or unauthorised use of computers, networks, and electronic data and against illicit access to or interception of data kept on these systems (Ikusika, 2022). In banking, cybersecurity refers to the defence of private financial data and systems against digital attacks which may span data breaches and financial fraud to advanced cyber espionage (Oluwatosin, Johnson, Femi, & Ogugua, 2024).

Given its elements of data protection, fraud detection, and prevention, cybersecurity is very essential for the existence of businesses (Ikuero & Zeng, 2022). Good data security guarantees private data against illegal access, therefore fostering customer confidence and regulatory compliance (Khalil, Manzoor, Tahir, Khan, & Jamal, 2021). By implementing robust cybersecurity measures, companies may prevent data breaches that can have legal consequences, financial losses, and damage of reputation (Kala, 2023). Moreover, methods of fraud detection and prevention are quite essential for spotting and lowering dishonest behaviour while safeguarding the financial integrity and resources of the company (Arcuri, Brogi, & Gandolfi, 2017). These cybersecurity techniques provide a secure and strong working environment that collectively guarantees the long-term survival of the company.

Although plethora of studies e.g., Oluwatosin et al., 2024; Akintoye et al., 2022; Too & Mutuku, 2023; Oluwatosin et al., 2024; Arcuri et al., 2017; Khalil et al., 2021; Anoke et al., 2021 have shown that cybersecurity influences organisational outcomes such as financial innovation, generic performance, financial performance and business sustainability. However, no study to the best of our knowledge had explored the influence of cybersecurity on firms' profitability and operation efficiency in the Nigeria context especially among money deposit banks. Against this backdrop, this study examined the effect of cybersecurity on operational efficiency and profitability of money deposit banks in Nigeria to further emphasise the need for these banks to protect people's funds from criminals trying to commit fraud by stealing customers' funds.

Meanwhile, profitability is defined as a company's capacity to make profits relative to its costs over a certain time period, reflecting financial health and efficiency (Reschiwati, Syahdina, & Handayani, 2020). Profit margins, which indicate the profit-to-revenue ratio, are often used to assess how successfully a firm expenses and maximises earnings (Puspitaningtyas, Toha, & Prakoso, 2023). Another approach views profitability as a return on investment (ROI), emphasising the efficacy of resource utilisation in producing profits (Dioha, Mohammed, & Joshua, 2018). Profitability may also be measured in terms of net income, which is the leftover profits after deducting all expenditures, taxes, and costs from total revenue, reflecting the overall financial performance of corporate operations (Odusanya, Yinusa, & Ilo, 2018).

Firm operational efficiency is the capacity of a company to effectively translate resources into products and services while optimising processes to maximise output and quality (Dildhani, Praveeni, & Fernando, 2019). It means making sure that actions support the more general organisational aims and tying operational operations with strategic goals (Barth, Berkovitch, & Israeli, 2023). Eliminating waste and inefficiencies is another definition of operational efficiency; lean operations and ongoing development help to increase performance by means of this emphasis (Abd-Elmageed, Abdel Megeid, & Riad, 2020). It is also assessed in terms of the company's capacity for quick response to changes in the market, therefore preserving competitiveness via operational agility and creativity (Hu, 2022).

1.1. Cybersecurity and Organisational Outcomes

By looking at the frequency and kinds of electronic fraud in Nigerian banks, Fatoki (2023) found important fraud kinds included computer viruses, hacking, phishing, pharming, and insider accounting fraud. The research underlined difficulties in stopping cybercrime and underlined its negative effects on banks; it also suggested remedies based on poll results from 557 bank staff members spread among six Nigerian institutions. By means of efficient risk management and bank monitoring, cybersecurity, according to Akintoye et al. (2022), greatly improves financial innovation in Nigerian deposit money banks, therefore implying a favourable link between strong cybersecurity policies and financial development. Information security breaches, according to Arcuri et al. (2017), lower stock returns; financial firms suffer more than other industries, especially from non-confidential assaults. Emphasising the need of cybersecurity in the commercial sustainability of Nigerian insurance companies, Therefore Anoke et al., (2021), underlined a clear positive link between cybersecurity investments and corporate resilience despite continuous cyber-attacks. Underlining the need of sophisticated cybersecurity measures in reducing fraud risks, Victory et al. (2022) underlined the efficiency of

cloud and application security in improving fraud prevention in Nigerian commercial banks. Taken together, this research highlighted the vital need of cybersecurity in preserving the integrity, creativity, and viability of Nigerian financial institutions among rising cyber hazards. Hence this study hypothesised that:

- ***H*1:** Cybersecurity has significant effect on operation efficiency of money deposit banks in Nigeria.
- ***H*2:** Cybersecurity has significant effect on profitability of money deposit banks in Nigeria.

1.2. Dynamic Capacities Theory

The Dynamic Capabilities Theory, put forth by Teece, Pisano, and Shuen, holds that a company's power to integrate, generate, and reconfigure internal and external resources and capabilities defines its competitive advantage in always shifting environments (Samsudin & Ismail, 2019). Three main capabilities recognising opportunities and hazards, seizing possibilities, and reorganising assets are the emphasis of this theory. Sensing is the method by which companies find probable disruptions and changes in the market, therefore helping them to forecast and respond to new threats and trends (Yi, Oh, & Amenuvor, 2023). Seizing focuses on organising resources to grab fresh opportunities, usually reached by means of innovative strategies and financial support (Nedzinskas, Pundziene, Buožiute-Rafanavičiene, & Pilkiene, 2013). Reconfiguring calls for constant updating and restructuring of the asset base of the company to remain current with the surroundings. Particularly in industries where technological innovations and market conditions are continually changing, these dynamic traits help companies to stay competitive, adjust, and grow (Bleady, Ali, & Ibrahim, 2018).

A relevant framework for looking at how cybersecurity affects the operational efficiency and profitability of Nigerian money deposit institutions is provided by the Dynamic Capabilities Theory. This concept highlights the requirement of banks always perceiving and seeing cyber threats so they may proactively put in place robust cybersecurity policies. Banks may utilise contemporary security solutions that not only protect their operations but also raise customer confidence and trust by using these opportunities, therefore improving profitability. Restructuring assets and capabilities also ensures banks' strength and flexibility to fit the always shifting landscape of cyber threats. By reducing disruptions and safeguarding sensitive data, this proactive approach to cybersecurity helps banks to maintain operational efficiency and hence build a lasting sustainability and a competitive edge in the financial sector.

2. Methodology

Design for the study is quantitative using cross-sectional research methods and surveys. Survey research is described as a way of gathering particular information from and about individuals in order to characterise, contrast and further explain their understandings, beliefs, and actions (Ojeleye, Abu-Abdissamad, Umar, & Usman, 2022). Using infinite population, Cochran's sampling method let one arrive at a sample size of 385. The research is a survey since Lagos state's money deposit banks distributed 385 pieces of questionnaires among their staff. Lagos state was selected as several banks in Nigeria have concentrated their head offices there. The research is also cross-sectional as the respondent's data were gathered point-in-time. The research is also cross-sectional as responders will be gathered at one-short or single point of contact. According to Sekaran and Bougie (2016), it is the compiling of information at one point in time to capture a moment of a certain phenomenon within a population. Google forms supplied the data electronically. Dillman, Smyth and Christian (2014), defined an online questionnaire as a wholly electronic survey dependent on internet source to get replies from participants. Out of the 385 pieces of questionnaire distributed, 372 (97%) were retrieved and used in the study.

2.1. Instrument

Adapted scales from previous studies were utilised in this study. Profitability was measured using Spillan and Parnell (2006) 4-items of the 9-item performance scale that are related to financial aspect of performance. Sample of item is “Return on investment goals have been achieved” with evaluated Cronbach’s alpha of 0.707. Operation efficiency was measured using 5-item operational efficiency scale of De Weerd-Nederhof, Visscher, Altena and Fisscher (2008) with reported Cronbach’s alpha of 0.83. sample of item is “Our development costs are lower than our competitors”. Cybersecurity was measured using the adapted 7-item scale of information security culture scale of Flores and Ekstedt (2016). Sample of item is “My coworkers caution me about dangerous email usage, virus downloads, or poor password choices” with reported Cronbach’s alpha of 0.89. All the constructs were measured on 5-points Likert scale ranging from 1- strongly disagree to 5- strongly agree.

3. Data Analysis and Presentation

Data were analysed using Structural Equation Model (SEM) particularly Smart-PLS 3.3.8 prior to conducting preliminary analysis such as missing values, outlier, common method variance and normality.

3.1. Analysis of Measurement Models

The measurement model also called inner model is often to ascertain the outer loadings, construct validity, reliability and coefficient of determination (R-square). The outer loading is often used to understanding the extent to which an item in a construct explains the variance or contribute to understanding the entire construct. Hair, Hult, Ringle and Sarstedt (2014) recommended the retention of outer loading of 0.7 and above and deletion of does below. They however, argued that loading of 0.4 and above can be retained if they do not have adverse effect on construct reliability and average variance extracted. Following the guideline loading of 0.5 and above were retained (See Table 1 & Figure 1 below). Additionally, the construct validity comprising of convergent and discriminant validity were assessed. Fornell and Larcker (1981) recommended the use of Average Variance Extracted (AVE) to confirm convergent validity. They recommended AVE value of 0.5 and above to establish convergent validity. Table 1 below depicted that the value of AVE for the two models is greater than 0.5. As such, convergent validity is confirmed.

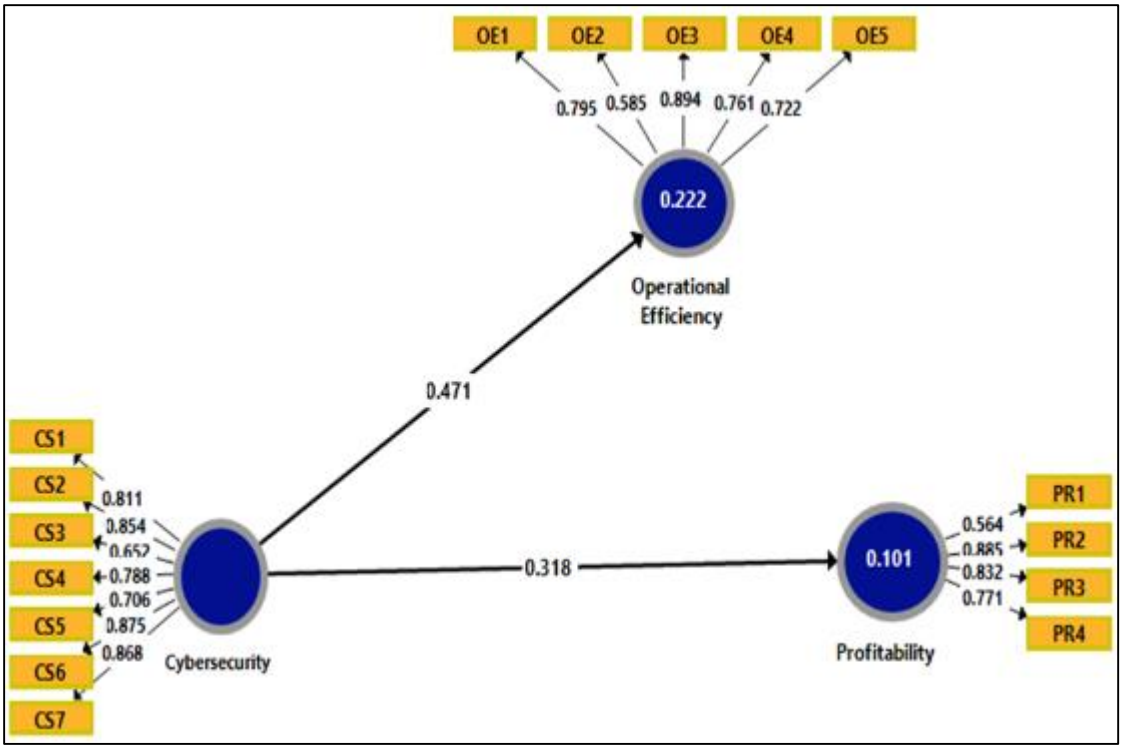

Figure 1 Measurement Model

Meanwhile, the reliability of the instrument was confirmed using composite reliability. Sekaran and Bougie (2016) recommended value of 0.7 and above to establish that the research instrument is consistent and adequate. Looking at Table 1 below all the values of the composite reliability is greater than 0.7. Hence, construct's reliability is established.

Table 1 Outer loadings, Reliability and Convergent Validity

Construct	Indicator	Outer loadings	Composite Reliability	AVE	Decision
Cybersecurity	CS1	0.811	0.924	0.636	Accepted
	CS2	0.854			
	CS3	0.652			
	CS4	0.788			

	CS5	0.706			
	CS6	0.875			
	CS7	0.868			
Operational Efficiency	OE1	0.795	0.869	0.575	Accepted
	OE2	0.585			
	OE3	0.894			
	OE4	0.761			
	OE5	0.722			
Profitability	PR1	0.564	0.853	0.597	Accepted
	PR2	0.885			
	PR3	0.832			
	PR4	0.771			
Source: Smart-PLS output (2024)					

Furthermore, Fornell and Larcker (1981) recommended their popular intercorrelation criterion to establish discriminant validity. They argued to confirm discriminant validity the square root of the AVE which depicts a construct's intercorrelation but be greater than the correlation with other constructs. Table 2 below showed the square root of AVE (bolded figure) is greater than intercorrelation with other constructs. Thus, discriminant validity is established.

Table 2 Fornell and Larcker Criterion for Discriminant Validity

Constructs	**Cybersecurity**	**Operational Efficiency**	**Profitability**
Cybersecurity	0.797		
Operational Efficiency	0.471	0.758	
Profitability	0.318	0.532	0.773
Source: Smart-PLS output (2024)			

Additionally, the Coefficient of Determination (R^2) values for Model 1 and Model 2 are 0.555 and 0.287, respectively (See: Figure 1 and Table 3 respectively). With a R^2 of 0.222 for Model 1, the independent factors clearly explain 22.2% of the variation in the dependent variable i.e., operational efficiency (OE), therefore indicating a quite excellent fit of the model and a modest to strong association. On the other hand, Model 2's R^2 of 0.101 reflects a smaller association and a modest fit and suggests that only 11.1% of the variation in profitability (PR) is explained by cybersecurity. Model 1 therefore shows greater general fit and more predictive ability than Model 2.

Table 3 Coefficient of Determination (R-Square)

Model 1	0.222	
Model 2	0.101	
Source: Smart-PLS output (2024).		

3.2. Analysis of Structural Models

The structural model also known as the outer model is utilised to ascertain the hypothesised relation.

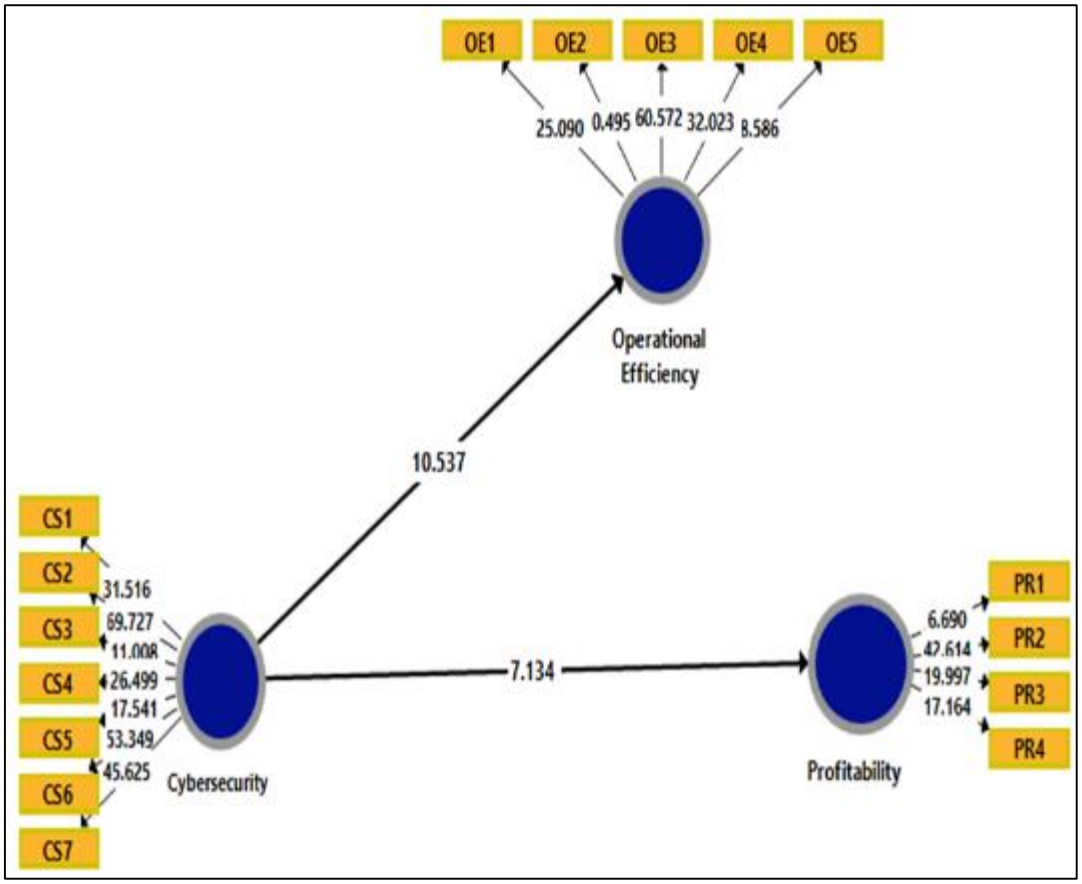

Figure 2 Structural Model

Table 4 Hypothesised Relationships

Hypotheses	Relationship	Beta	Standard Deviation	T Statistics (|O/STDEV|)	P Values	Decision
***H*1**	Cybersecurity -> Operational Efficiency	0.471	0.045	10.537	0.000	Supported
***H*2**	Cybersecurity -> Profitability	0.318	0.045	7.134	0.000	Supported
Source: Smart-PLS output (2024).						

Investigating the hypothesised relationships shows significant favourable effects of cybersecurity on operational efficiency and profitability in hypotheses 1 and 2. With a beta coefficient of 0.471, a standard deviation of 0.045, and a T statistic of 10.537, with a p-value of 0.000, cybersecurity and operational efficiency have a significant link in first hypothesis. This shows that improvements in cybersecurity techniques significantly increase operational efficiency of money deposit banks in Nigeria, most likely by lowering the danger of cyber-attacks and guaranteeing better, more consistent operational procedures.

In the second hypothesis. with a beta coefficient of 0.318, a standard deviation of 0.045, and a T statistic of 7.134 along with a p-value of 0.000, cybersecurity similarly favourably affects profitability. This link emphasises the financial advantages of strong cybersecurity policies as it implies that investments in cybersecurity not only guard against losses from cyber events but also help the general financial performance of the company. At the 0.000 level, these associations are statistically significant, therefore verifying the strong and dependability of the favourable effects of cybersecurity on operational efficiency and profitability.

4. Discussions

Operating efficiency of Nigerian money deposit banks is much enhanced by cybersecurity in general. Strong cybersecurity protects banks from disruptive cyberattacks, therefore guaranteeing consistent operations (Victory et al., 2022). Cybersecurity increases financial system efficiency by minimising breaches and lowering downtime, therefore enabling seamless transaction flows and ongoing service delivery (Anoke et al., 2021). Strong cybersecurity also instills customer trust, which drives the adoption of digital banking products, thus streamlining procedures (Akintoye et al., 2022). This defence also reduces the risk of financial losses brought on by fraud and replaces the need for costly reactive measures (Oluwatosin et al., 2024). Consequently, banks may focus on important development initiatives, better control resources, and maintain their competitive edge in the financial sector.

Cybersecurity has a positive and significant impact on the profitability of Nigerian money deposit banks. Strong cybersecurity policies help to prevent costly data breaches and fraud, therefore reducing financial losses and the expenses of addressing such events (Ojeka et al., 2017). Banks build loyalty and confidence by protecting private client data and preserving transaction integrity, therefore strengthening customer retention and appeal (Oluwatosin et al., 2024). Moreover, good cybersecurity might help the bank stand out from competitors, boost its reputation, and maybe attract more business (Fatoki, 2023). These components enable banks to focus on income-generating expansion plans and innovations as they serve to provide a stable and safe operating environment (Too & Mutuku, 2023). All things considered, strong cybersecurity systems guard financial resources and provide the foundation for long-term profitability and business success.

4.1. Implications

The findings have broad practical relevance on how cybersecurity affects operating efficiency and profitability of Nigerian money deposit banks. These findings underline the significance of always monitoring systems and building robust cybersecurity architecture to prevent cyberattacks. By minimising disruptions and raising general efficiency, advanced security measures may simplify procedures. From a profitability standpoint, these cybersecurity costs minimise financial losses from fraud and breaches as well as boost consumer confidence and loyalty all of which are very vital for the survival of the business. Moreover, governments and authorities might use these results to demand institutions to use best practices and enforce more strict cybersecurity rules, therefore strengthening the financial system. All things considered, giving cybersecurity first priority not only guards banks' assets but also supports long-term operational and financial stability, thereby benefiting the broader economy.

Based on the Dynamic Capabilities Theory, the theoretical consequences of the findings highlight the importance of adaptive and proactive cybersecurity measures in increasing the operational efficiency and profitability of Nigerian money deposit banks. This concept holds that banks have to constantly develop their dynamic capacity for perceiving, grabbing, and reorganising resources in response to evolving cyber threats. The findings of the research confirm the idea that cybersecurity is a strategic ability that helps organisations to effectively negotiate a constantly changing threat environment rather than just a technical need. Strong cybersecurity policies will help banks to better detect prospective attacks early on, implement suitable responses, and modify their security architecture to prevent future threats. Being consistent with the Dynamic Capabilities Theory highlights the need of developing an organisational culture that gives constant learning, inventiveness, and adaptability in cybersecurity practices top priority, so producing long-term success and ongoing competitive advantage in the financial sector.

5. Conclusion and Recommendations

In sum, the study underscores the need of cybersecurity in raising the operational profitability and efficiency of Nigerian money deposit banks. It is abundantly evident from aligning with the Dynamic Capabilities Theory that banks have to address cybersecurity actively and adaptably if they are to effectively control and reduce rising cyber risks. The findings underline the need of strong cybersecurity policies in not only preventing operational delays and financial losses but also in building consumer confidence and loyalty, hence promoting long-term profitability and corporate viability. Preserving a competitive edge and guaranteeing the financial sector's resilience therefore depend on ongoing improvement of security procedures and investment in contemporary cybersecurity infrastructure.

The findings provide two recommendations for Nigerian money deposit banks.

- Money deposit banks should give constant investment in advanced cybersecurity technologies and knowledge top priority. This entails enhancing detection and reaction strategies to promptly handle fresh cyber threats, thus safeguarding operations and customer data.

- At all levels of the banks, developing a culture of cybersecurity awareness and training is very vital. This ensures that staff members can see and control potential hazards, therefore boosting general cyber catastrophe resilience. Following these policies will enable banks to maintain profitability in the face of a challenging and rising threat environment, improve operational efficiency, and increase their cybersecurity posture.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abd-Elmageed, M. H., Abdel Megeid, N. S., & Riad, N. M. A. H. (2020). Impact of Operational Efficiency and Financial Performance on Capital Structure using Earnings Management as a Moderator Variable. *Accounting Thought*, *24*(3), 1029–1059. https://doi.org/10.21608/atasu.2020.160431

[2] Akintoye, R., Ogunode, O., Ajayi, M., & Joshua, A. A. (2022). Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria. *Universal Journal of Accounting and Finance*, *10*(3), 643–652. https://doi.org/10.13189/ujaf.2022.100302

[3] Anoke, A. F., Igwebuike, Joyce, Agagbo Ogugua, C., & Odumuato, V. (2021). Cyber Security and Business Sustainability of Quoted Insurance Firms in Nigeria. *Journal of Research in Business and Management*, *9*(12), 16–22.

[4] Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). How does cyber crime affect firms? The effect of information security breaches on stock returns. *CEUR Workshop Proceedings*, *1816*(2015), 175–193.

[5] Barth, M. E., Berkovitch, J., & Israeli, D. (2023). The information content of operational efficiency. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4558856

[6] Bleady, A., Ali, A. H., & Ibrahim, S. B. (2018). Dynamic capabilities theory: Pinning down a shifting concept. *Academy of Accounting and Financial Studies Journal*, *22*(2), 1–16.

[7] De Weerd-Nederhof, P. C., Visscher, K., Altena, J., & Fisscher, O. A. M. (2008). Operational effectiveness and strategic flexibility: Scales for performance assessment of new product development systems. *International Journal of Technology Management*, *44*(3–4), 354–372. https://doi.org/10.1504/IJTM.2008.021044

[8] Dildhani, A. K. D. N., Praveeni, S. M. N., & Fernando, J. A. A. N. (2019). Factors Affecting on Operational Efficiency. *Symposium Proceedings of Vavuniya Campus Research Symposium 2019*, (October), 45–50. Retrieved from http://www.vau.jfn.ac.lk/vcirs2019/wp-content/uploads/2019/09/Proceedings-VCIRS-2019.pdf#page=56

[9] Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, Phone, Mail and Mixed-Mode Surveys: The Tailored Design Method* (4th ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.

[10] Dioha, C., Mohammed, N. A., & Joshua, O. (2018). Effect of Firm Characteristics on Profitability of Listed Consumer Goods Companies in Nigeria Dioha Charles. *Journal of Accounting, Finance and Auditing Studies*, *4*(2), 14–31.

[11] Fatoki, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. *International Journal of Science and Research Archive*, *9*(2), 503–515. https://doi.org/10.30574/ijsra.2023.9.2.0609

[12] Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, *59*, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

[13] Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research.*, *18*(1), 39–50.

[14] Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2014). Partial least squares structural equation modeling (PLS-SEM). *Sage Publisher*. https://doi.org/10.1108/EBR-10-2013-0128

[15] Hu, R. (2022). Evaluation of Operating Efficiency of Small and Medium Sized Technology Enterprises based on DEA Model: A Case Study of Jiangsu Province. *Proceedings of the 2022 2nd International Conference on Enterprise*

Management and Economic Development (ICEMED 2022), *656*(Icemed), 530–533. https://doi.org/10.2991/aebmr.k.220603.084

[16] 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://doi.org/10.4314/njt.v41i3.10

[17] Ikusika, B. (2022). *A Critical Analysis of Cybersecurity in Nigeria and the Incidents of Cyber-Attacks on Businesses/Companies* (Nigerian Law School). Nigerian Law School. Retrieved from https://ssrn.com/abstract=4165204

[18] Kala, E. M. (2023). The Impact of Cyber Security on Business: How to Protect Your Business. *Open Journal of Safety Science and Technology*, *13*(02), 51–65. https://doi.org/10.4236/ojsst.2023.132003

[19] Khalil, K., Manzoor, S. R., Tahir, M., Khan, N., & Jamal, K. (2021). Impact of Cyber Security Cost on the Financial Performance of E-Banking: Mediating Influence of Product Innovation Performance. *Humanities & Social Sciences Reviews*, *9*(2), 691–703. https://doi.org/10.18510/hssr.2021.9266

[20] Nedzinskas, Š., Pundziene, A., Buožiute-Rafanavičiene, S., & Pilkiene, M. (2013). The impact of dynamic capabilities on SME performance in a volatile environment as moderated by organizational inertia. *Baltic Journal of Management*, *8*(4), 376–396. https://doi.org/10.1108/BJM-01-2013-0003

[21] Odusanya, I. A., Yinusa, O. G., & Ilo, B. M. (2018). Determinants of firm profitability in Nigeria: Evidence from dynamic panel models. *Journal of Economics and Business*, *68*(1), 43–58. Retrieved from http://hdl.handle.net/10419/195210

[22] Ojeka, S. A., Ben-Caleb, E., & Ekpe, I. (2017). Cyber security in the Nigerian banking Sector: An Appraisal of audit committee effectiveness. *International Review of Management and Marketing*, *7*(2), 340–346. Retrieved from http:www.econjournals.com

[23] Ojeleye, Y. C., Abu-Abdissamad, A. M., Umar, S., & Usman, A. (2022). Academic resilience and self- efficacy as predictors of students' academic performance in Nigeria. *Sokoto Journal of Management Studies*, *32*(3), 97–112.

[24] Oluwatosin, R., Johnson, S. O., Femi, O., & Ogugua, C. O. (2024). Cybersecurity Dynamics in Nigerian Banking: Trends and Strategies Review. *Computer Science & IT Research Journal*, *5*(2), 336–364. https://doi.org/10.51594/csitrj.v5i2.761

[25] Puspitaningtyas, Z., Toha, A., & Prakoso, A. (2023). Understanding the concept of profit as an economic information instrument: disclosure of semantic meanings. *Accounting and Financial Control*, *2*(1), 27–36. https://doi.org/10.21511/afc.02(1).2018.03

[26] Reschiwati, R., Syahdina, A., & Handayani, S. (2020). Effect of liquidity, pofitability, and size of companies on firm value. *Utopía Y Praxis Latinoamericana*, *25*(6). https://doi.org/10.5281/zenodo.3987632

[27] Samsudin, Z. binti, & Ismail, M. D. (2019). The Concept of Theory of Dynamic Capabilities in Changing Environment. *International Journal of Academic Research in Business and Social Sciences*, *9*(6), 1071–1078. https://doi.org/10.6007/ijarbss/v9-i6/6068

[28] Sekaran, U., & Bougie, R. (2016). *Research Method for Business: A Skill Building Approach* (7th ed.). Chichester: John Wiley & Sons Ltd.

[29] Spillan, J., & Parnell, J. (2006). Marketing resources and firm aerformance Among SMEs. *European Management Journal*, *24*(2–3), 236–245. https://doi.org/10.1016/j.emj.2006.03.013

[30] Too, W. K., & Mutuku, M. (2023). An examination of the effects of cyber security in enhancing performance of the public sector institutions: Literature review. *Reviewed Journal International of Business Management*, *4*(1), 471–477. https://doi.org/10.61426/business.v4i1.141

[31] Victory, C. O., Promise, E., & Mike, C. N. (2022). Impact of Cyber-Security on Fraud Prevention in Nigerian Commercial Banks. *Jurnal Akuntansi, Keuangan, Dan Manajemen*, *4*(1), 15–27. https://doi.org/10.35912/jakman.v4i1.1527

[32] Yi, H. T., Oh, D., & Amenuvor, F. E. (2023). The effect of SMEs' dynamic capability on operational capabilities and organisational agility. *South African Journal of Business Management*, *54*(1). https://doi.org/10.4102/sajbm.v54i1.3696