TPM Vol. 32, No. S3, 2025
ISSN: 1972-6325
https://www.tpmap.org/

CYBERSECURITY AS AN INTERACTIVE VARIABLE BETWEEN BANKING FINANCIAL RISK MANAGEMENT AND DIGITAL CUSTOMER SERVICES

HA IDAR HAMOUDI ALI AL ZUBAIDI
FACULTY OF ADMINISTRATION AND ECONOMICS, KUFA UNIVERSITY, NAJAF, IRAQ
EMAIL: haidarh.alzubaydi@uokufa.edu.iq
ORCID ID: HTTPS://ORCID.ORG/0009-0003-8520-6066

ALI ZAIDAN FENJAN
UNIVERSITY, NAJAF, IRAQ,
EMAIL: aliz.alsharmani@uokufa.edu.iq
ORCID: ORG/ 0009-0006-2716-5173

WISAM NEAMAH RAGEEB
FACULTY OF ADMINISTRATION AND ECONOMICS, KUFA UNIVERSITY, NAJAF, IRAQ,
EMAIL: wisamn.rgeeb@uokufa.edu.iq
ORCID ID: HTTPS://ORCID.ORG/0009-0005-1738-9977

AKRAM SAMI FAYEZ
BUSINESS ADMINISTRATION DEPARTMENT- UNIVERSITY OF BASRAH – IRAQ
EMAIL: pgs.akram.sami@uobasrah.edu.iq
ORCID ID: HTTPS://ORCID.ORG/0009-0008-3744-1877

MOHAMMED HAMEED YASIR
FACULTY OF ADMINISTRATION AND ECONOMICS, KUFA UNIVERSITY, NAJAF, IRAQ,
EMAIL: MOHAMMEDH.ALHCHEMEY@UOKUFA.EDU.IQ.
ORCID ID HTTPS://ORCID.ORG/0009-0001-4716-2483

ABSTRACT

The current study derives its significance from the importance of the commercial banking sector, which is the cornerstone of the economy and the driver of corporate financing operations. This study aims to diagnose and test the relationship between variables of financial risk management and digital customer services in the Iraqi commercial banking sector, while analyzing the role of cybersecurity as an interactive variable in this relationship. This study is deemed essential due to the increasing reliance on digital platforms and the rising cyber threats that necessitate robust strategies to ensure service continuity, security, reliability, and trust.

The study adopted a descriptive analytical approach for data analysis and interpretation. A questionnaire was used to collect data, with (351) forms distributed, and the study was conducted on a sample of (18) commercial banks. The sample included various levels of upper, middle, and executive management. A set of statistical methods and tools was utilized, including Excel, Smart PLS4. The results of the descriptive analysis demonstrated that the surveyed banks possess Banking Financial Risk Management while simultaneously working to enhance the Digital Customer Services. Furthermore, the results indicated positive trends concerning cybersecurity. The statistical analysis results revealed a significant relationship between Banking Financial Risk Management and the Digital Customer Services, as well as an interactive role of Cybersecurity between the research variables.

Keywords: Banking sector, Banking Financial Risk Management, Digital Customer Services, Cybersecurity .

INTRODUCTION

The increasing reliance of the banking sector in recent years on digital services has made it essential to enhance cybersecurity to protect sensitive data from unauthorized access. In the context of financial risk management, this includes identifying and assessing the risk priorities that financial institutions may face, as well as controlling the negative impacts of those risks by developing risk management strategies to achieve banking stability. (fischer,2016:7)
Banks focus on serving digital customers with the aim of improving high-quality digital services in the economic sector, in order to enhance business efficiency amidst the significant expansion of digital transformation and increased digital competition among banks. Consequently, the quality of economic services has become a fundamental factor in achieving sustainable competitive advantage, thereby supporting and enhancing the efficiency of financial sectors. (Huang etal , 2024:861)
In light of the banks' shift from traditional operations to those based on digital systems, the need for effective management of financial banking risks arising from digital failures or thefts is increasing.. (Kochovski et al., 2019: 16)
The continuity of the bank in providing digital services in a reliable and robust manner depends on cybersecurity amidst a rapidly evolving environment of cyber threats. The rapid advancement in financial technology has increased the interaction of individuals, organizations, and banks with financial services. Thus, the benefits of digital transformation are accompanied by significant challenges, particularly concerning cybersecurity threats to banks. The knowledge gap in the current study lies in the notable lack of studies addressing the relationship between financial risk management in banking, digital customer services, and cybersecurity, due to the absence of integrated theoretical frameworks and weak empirical evidence on how cybersecurity influences the reduction of financial risks associated with key economic services, particularly in the Iraqi banking sector. Furthermore, there is a scarcity of studies measuring dimensions of digital quality such as security, speed, and responsiveness in reducing financial risks in emerging digital environments that rely on systems not fully protected from cyberattacks.
The challenges facing bank management require the adoption of robust cybersecurity strategies to protect sensitive data, ensure service continuity, and enhance trust among users of digital financial services. (Fisher, 2016: 7)
Cybersecurity is an essential part of multi-service business management, relying on the ability to anticipate, respond to, and adapt to cyber events. In the context of digital financial services, this becomes an important factor in protecting transactions and user information with the programming of financial platforms. (colmann, 2011: 5) The current study examines the interests of cybersecurity as key variables in multi-service financial management in the financial sector, and its implications for the provision of economic services to people. It also explores how to study the effectiveness of digital security in various fields and the quality of services provided to customers.

SCIENTIFIC METHODOLOGY OF THE STUDY

1.1 RESEARCH PROBLEM

This study seeks to understand how cybersecurity, as an interactive variable, affects financial risk management in commercial banks and how this can impact the quality of banking services provided to customers. With technological advancements and increasing cyber threats, it has become necessary to study how banking cybersecurity interacts with financial risk management to improve digital customer services. Therefore, the research problem lies in how banking financial risk management impacts the quality of economic services in light of current cyber challenges.

1.2 RESEARCH OBJECTIVES

The current research aims to study the interactive role of cybersecurity in the relationship between financial risk management and digital customer services, which represent the new competitive advantage for banks in the current era. Furthermore, it aims to highlight the importance of financial risk management in enhancing the financial stability of banks. The research seeks to help banks avoid cybersecurity threats by strengthening cybersecurity measures to adapt to these digital threats and risks.

1.3 IMPORTANCE OF THE RESEARCH

The current research aims to demonstrate the importance of applying its variables: banking financial risk management, digital customer services, and cybersecurity. It also examines the availability of infrastructure and physical and human resources in commercial banks. It also aims to analyze the impact of banking financial risk management on digital customer services and explore the relationship between cybersecurity and banking financial risk management.

1.4 RESEARCH HYPOTHESES

H1: There is a statistically significant impact relationship between Banking Financial Risk Management and the Digital Customer Services of the commercial banks in the research sample.

H2: There is a statistically significant impact relationship between Banking Financial Risk Management and the Digital Customer Services through the interactive effect of Cybersecurity of the commercial banks in the research sample.

2. THEORETICAL FRAMEWORK OF THE STUDY

2.1 BANKING FINANCIAL RISK MANAGEMENT

Banking risks represent the potential financial losses resulting from a customer's inability to meet their obligations. Successful banks operate according to a clear strategy based on the success or failure of their companies, while risk management approaches vary from company to company, depending on the availability of sufficient data to facilitate understanding of appropriate procedures.

The meaning of risks corresponds to the meaning of material and moral losses that occur due to an event with the presence of contributing factors. They are considered phenomena of economics and management. The intensity of risks has increased for two reasons: the first is the increase in changes that have occurred in the internal and external environment, and the second is the diversification and expansion of economic activities, which has become a hallmark of contemporary economies. (Sithipolvanichgul, 2016:16) Consequently, there is a connection between risks and rapid environmental changes as well as economic diversification. On the other hand, businesses in general, and commercial banks in particular, cannot avoid these risks, which will reflect on their business results and activities, in addition to exposing them to failure and threats to the continuity of their operations. (Rampini etal, 2016:5)

Risk management is defined as the uncertainty in making financing and investment decisions, profit distribution, and determining acceptance and rejection decisions. Furthermore, risk management includes identifying the potential size of investment losses and then taking appropriate action based on investment objectives and the risk tolerance of the investor. It is also defined as identifying potential events that may affect the company's cash flows and reducing the impact of these events on cash flows.

Risk management includes four main dimensions, starting with understanding the risks that companies must recognize and formulating a clear perception of all risk-causing factors. It involves defining risks that represent unpredictable events, which, when they occur, expose the company to problems. Furthermore, risk assessment requires the company to conduct a continuous evaluation of these risks in terms of their severity and likelihood of occurrence. Finally, risk monitoring and control involve overseeing and tracking the measures taken by the company and any other potential deviations that may arise.(Stulz,2016 :48) Accordingly, there is a set of strategies employed for risk management. Building a robust risk management strategy enables the company to understand and analyze risks, then find solutions that mitigate the severity of those risks. The strategies employed for risk management include the transfer strategy, which helps the bank accept risks from another party; the avoidance strategy, which the company implements to avoid activities that lead to potential hazards; the mitigation strategy, which reduces the severity of losses resulting from risks; and finally, the acceptance strategy, under which the company chooses to accept losses when they occur. (Nanda,2024:22)

2.2 DIGITAL CUSTOMER SERVICES

It means using digital technology to direct reasons online or through mobile applications. The quality of these services is essential to effectively meet the needs of users, especially in marginalized communities. High-quality digital economic services can lead to improved access to official economic accounts, reduced transaction costs, and enhanced customer satisfaction. (Sharma, & Díaz Andrade, 2023: 586). Digital customer services have improved access for vulnerable groups to economic resources. By facilitating access to formal accounts and reducing the costs of financial transfers, these services contribute to alleviating poverty and enhancing financial stability in marginalized communities. This impact underscores the importance of maintaining the quality of services to ensure that the benefits of digital financing are widely distributed. (Ozili, 2018: 349) The Digital Customer Services refers to the effectiveness, efficiency, and user satisfaction with these services. High-quality digital economic services meet customer expectations, ensure reliability, and create value for individuals and companies (Luo, et al, 2022: 18).

The aim of digital customer services is to achieve efficiency and effectiveness in the economic services provided through digital means to meet customer needs and expectations. With the rapid advancements in financial technology (FinTech), the quality of digital services has become a critical factor in the success of economic institutions in the market (Bapat, 2022: 305).

The main dimensions of the Digital Customer Services include accessibility and customer support. This dimension refers to the availability of digital economic services to users, particularly marginalized groups (Madueke& Eyupoglu,2024:5). It includes factors such as the geographical scope of services and the existing technological infrastructure. Ensuring broad access is essential for enhancing financial inclusion and empowering users to benefit from digital economic services. (Bankuoru Egala, et al, 2021: 148)

The usage dimension measures the frequency and effectiveness of user interactions with digital economic services. It reflects the actual adoption and utilization of these services by consumers. High usage rates indicate that the services meet user needs and integrate into their financial behaviors. (Vo ,etal,2020: 505)

Finally, data quality focuses on the accuracy, completeness, and reliability of the data used in digital economic services. This is critical for effective decision-making and risk management. Poor data quality can lead to significant operational risks and undermine customer trust in financial services. Quality encompasses various aspects of service delivery, including reliability, security, and user experience. It also includes the service's responsiveness to user inquiries and issues High-quality services enhance user trust and satisfaction.

2.3 CYBERSECURITY

,Cybersecurity represents a structured and disciplined approach that aligns strategy, operations, individuals (.technology, and knowledge with the objective of managing the uncertainties faced by banksManab etal,2010:242) The European Systemic Risk Board (ESRB), which oversees the financial system of the European Union, has identified cyber risks as "a source of systemic risk to the financial system" (ESRB 2020) A set of activities and ,measures aimed at protection against attacks, sabotage, or other threats faced by computer systems, computer checks .related devices, software, and the information contained within and communicated by them(Fischer,2014) based on the fear that a cyber-security incident could escalate, creating a liquidity crisis that would erode the confidence of economic actors and destabilize the entire system (Greenberg,2020:6). Liquidity is a buffer and stabilizing factor for banks, ensuring the banking system's ability to meet credit requirements at all times (Al Zubaidi et al., 2025).To understand how cyber risks can generate such devastating shocks to the critical infrastructure we rely on, let us consider the widely reported case of the Danish shipping giant APM-Maersk. What is particularly interesting here is not the identification of the attackers or what this attack says about the current state of cyber conflict (Arquilla and Ronfeldt, 2007; Rid, 2012; Rid and Buchanan, 2015), but rather the extent of the destruction caused by such incidents even for the largest and most mature organizations, and how victims are upgrading their traditional cyber security risk management model to embrace a resilience model.(Ritchie,2019:2).

The concept of resilience remains marginal in the literature related to cyber risks. When it does appear, it primarily arises in the field of computer science, where key research questions relate to identifying the engineering traits that can make cyber systems more robust and the metrics that can be used to assess their resilience (Bodeau and Graubart, 2011; Linkov et al., 2013). While these matters are important, there is a need for a more comprehensive approach to help understand the types of preparedness, responses, recovery, and adaptation activities necessary to enhance an organization's Cybersecurity (The National Academies, 2012).

Cybersecurity can be defined as "the ability to achieve the intended outcome despite ongoing adverse cyber events" (Björk et al., 2015: 312). This definition distinguishes Cybersecurity from cybersecurity, whose primary goal is to predict and prevent harmful events.

Cybersecurity also refers to an organization's ability to prepare for, respond to, and recover from cyber incidents while maintaining core functions (Annarelli & Palombi, 2021: 14).

The importance of Cybersecurity in digital services is particularly pronounced in the financial sector, which is especially vulnerable to cyber threats that can lead to significant operational disruptions and financial losses. The increasing complexity of these attacks necessitates a robust Cybersecurity strategy that focuses not only on prevention but also on recovery and adaptation. This dual focus helps improve the Digital Customer Services by ensuring that organizations can maintain service continuity even in the face of cyber incidents (Petrenko, 2022: 159)

The Digital Customer Services is influenced by several factors, including data integrity, customer experience, and its role in promoting financial inclusion. As the digital financial landscape continues to evolve, focusing on these aspects will be crucial to maximizing the benefits of these services for all users (Yadav, 2023: 57). The implementation of effective Cybersecurity measures can lead to numerous positive outcomes for digital economic services (Dupont, 2019: 34).

RESULTS

STATISTICAL DESCRIPTION OF THE RESEARCH VARIABLES

The demographic composition of the respondents shows gender (56.3% males and 43.7% females); most of the respondents are aged between 27 and 56 years, have university education (6.7% master's, 64.4% bachelor's and 28% diploma), (37.4%) have worked more than 10 years, and (62.6%) have worked more than 10 years in the banks surveyed, respectively.

Table 1
Statistical Description

Code	Items	Mean	Standard Deviation	Kurtos-is	Skewn-ess
FRM1	How severe are the types of financial risks currently facing your bank?	3.56	1.18	-0.97	-0.32
FRM2	To what extent do you approve of the efficiency of your bank's credit risk management?	3.44	1.22	-1.08	-0.26
FRM3	How effective is the regulatory environment in supporting banking risk management?	3.44	1.15	-0.85	-0.30
FRM4	To what extent do political and economic factors impact your bank's financial risks?	3.64	1.26	-0.96	-0.52
FRM5	To what extent does your bank utilize modern technologies in risk management?	3.63	1.15	-1.02	-0.38
FRM6	How difficult are the challenges facing your bank's risk management?	3.50	1.23	-0.90	-0.41
FRM7	How important is it to enhance customer confidence in light of the current financial risks?	3.59	1.26	-1.07	-0.46
FRM8	How important is it to improve your bank's risk management systems?	3.58	1.28	-0.99	-0.48
Banking Financial Risk Management		**3.53**	**3.55**	**1.22**	**-0.98**
QDS1	How easy is it to use your bank's digital platforms (mobile app/website) to complete daily banking tasks?	3.50	1.26	-0.96	-0.39
QDS2	How satisfied are you with the speed of transaction processing across digital channels?	3.71	1.31	-0.85	-0.66
QDS3	To what extent do digital service options meet all your banking needs?	3.67	1.15	-0.99	-0.43
QDS4	How accurate and reliable is the financial information presented across digital channels?	3.64	1.14	-0.47	-0.59
QDS5	How effective is technical support in resolving digital banking issues?	3.60	1.24	-1.11	-0.42
QDS6	How responsive is the bank to customer feedback to improve digital services?	3.57	1.23	-0.82	-0.49
QDS7	How frequently do technical glitches hinder your digital banking experience?	3.72	1.16	-0.32	-0.71
Digital Customer Services		**3.63**	**3.63**	**1.21**	**-0.79**
CR1	How effective are your bank's measures in preventing cyberattacks?	3.60	1.29	-0.82	-0.61
CR2	To what extent do you feel your financial data is protected when using digital services?	3.54	1.29	-0.96	-0.50
CR3	How quickly does your bank respond when security threats are detected?	3.62	1.09	-0.79	-0.45
CR4	Are you adequately educated about secure digital service practices?	3.56	1.19	-1.09	-0.30
CR5	How often are you exposed to online fraud attempts through your bank's services?	3.57	1.21	-1.17	-0.34

CR6	How do you rate the level of encryption used to protect your transactions?	3.67	1.14	-0.98	-0.46
CR7	Do additional security measures impact your digital experience?	3.59	1.13	-0.79	-0.41
CR8	How confident are you in your bank's ability to recover from cyberattacks?	3.86	1.26	-0.68	-0.77
Cybersecurity		**3.63**	**3.63**	**1.20**	**-0.91**

Table (1) shows the average rating for the main dimensions of banking services (financial risk management, digital customer service, and cybersecurity), with averages ranging from 3.53 to 3.63, indicating significant room for improvement despite some positive points. Despite relative confidence in the targeted banks' ability to recover from cyber attacks, the results reveal clear challenges, including technical challenges and data integrity concerns. The high standard deviation also reflects significant variability in customer opinions, underscoring the urgent need to improve service quality and ensure a more stable and reliable customer experience. These results demonstrate that the bank's current performance requires comprehensive development to enhance operational efficiency and customer satisfaction.

2.4 Confirmatory Factor Analysis: Below are the results of the confirmatory factor analysis of the study variables, where we adopted the value (0.05) to retain the items without deleting them.

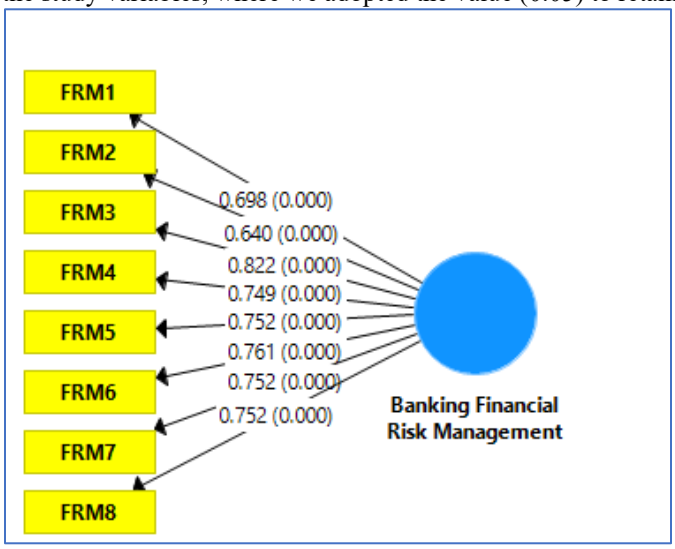

Fig 1. Factor analysis of Banking Financial Risk Management variable.

The results of Figure (1) which included the confirmatory factor analysis of Banking Financial Risk Management variable indicate that the questionnaire items (8) achieved factor saturation coefficients that fall within the statistically acceptable limits, as all items exceeded the approved minimum for factor saturation coefficients, indicating that these items measure the targeted dimension with a sufficient degree of internal consistency, as well as the acceptable (P-value), which was less than (0.05) for all items. Since excluding them does not significantly improve the quality of the model, and based on the above, the structural model can be considered valid and suitable for use in the analysis stages and subsequent statistical procedures.

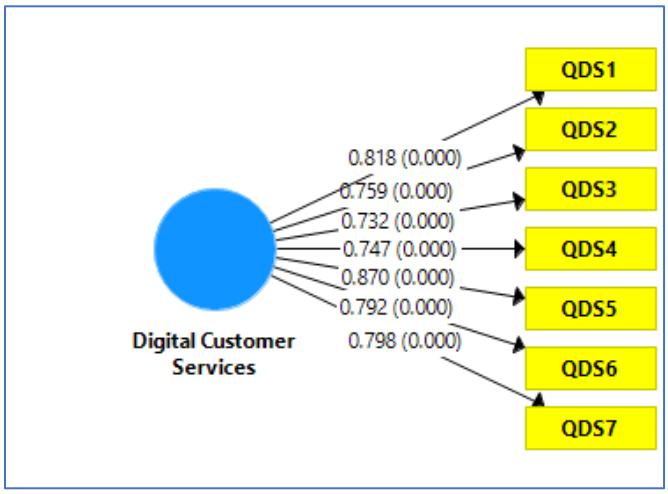

Fig 2. Factor analysis of Digital Customer Services variable.

The results of Figure (2) which included the confirmatory factor analysis of the of Digital Customer Services variable indicate that the questionnaire items (7) achieved factor saturation coefficients that fall within the statistically acceptable limits, as all items exceeded the approved minimum for factor saturation coefficients, indicating that these items measure the targeted dimension with a sufficient degree of internal consistency, as well as the acceptable (P-value), which was less than (0.05) for all items. Since excluding them does not significantly improve the quality of the model, and based on the above, the structural model can be considered valid and suitable for use in the analysis stages and subsequent statistical procedures.

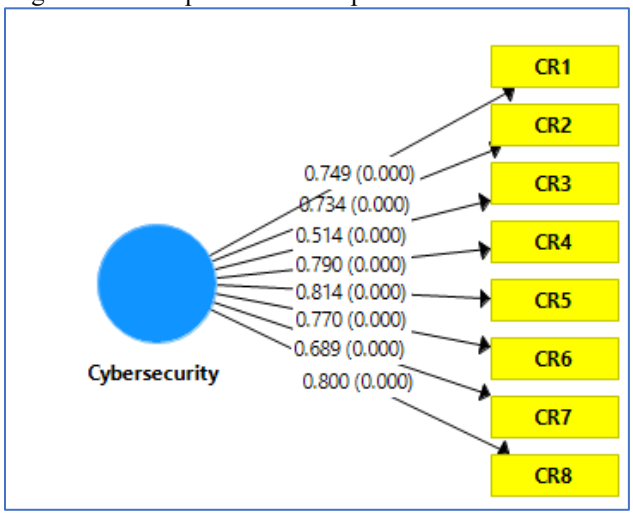

Fig 3. Factor analysis of Cybersecurity variable.

The results of Figure (3) which included the confirmatory factor analysis of the of Cybersecurity variable indicate that the questionnaire items (8) achieved factor saturation coefficients that fall within the statistically acceptable limits, as all items exceeded the approved minimum for factor saturation coefficients, indicating that these items measure the targeted dimension with a sufficient degree of internal consistency, as well as the acceptable (P- value), which was less than (0.05) for all items. Since excluding them does not significantly improve the quality of the model, and based on the above, the structural model can be considered valid and suitable for use in the analysis stages and subsequent statistical procedures.

IMPACT ANALYSIS OF STUDY VARIABLES

The following Figures and Tables present the regression analysis results for the study variables, examining their relationships and predictive effects.

2.4.1 Regression Analysis of Banking Financial Risk Management and Digital Customer Services

The table and figure present the results of a regression analysis to examine the effect of Banking Financial Risk Management on Digital Customer Services.

Table 2 Regression analysis test for Banking Financial Risk Management and Digital Customer Services variable

Variables	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Values
Banking Financial Risk Management -> Digital Customer Services	0.839	0.84	0.021	40.436	0.00

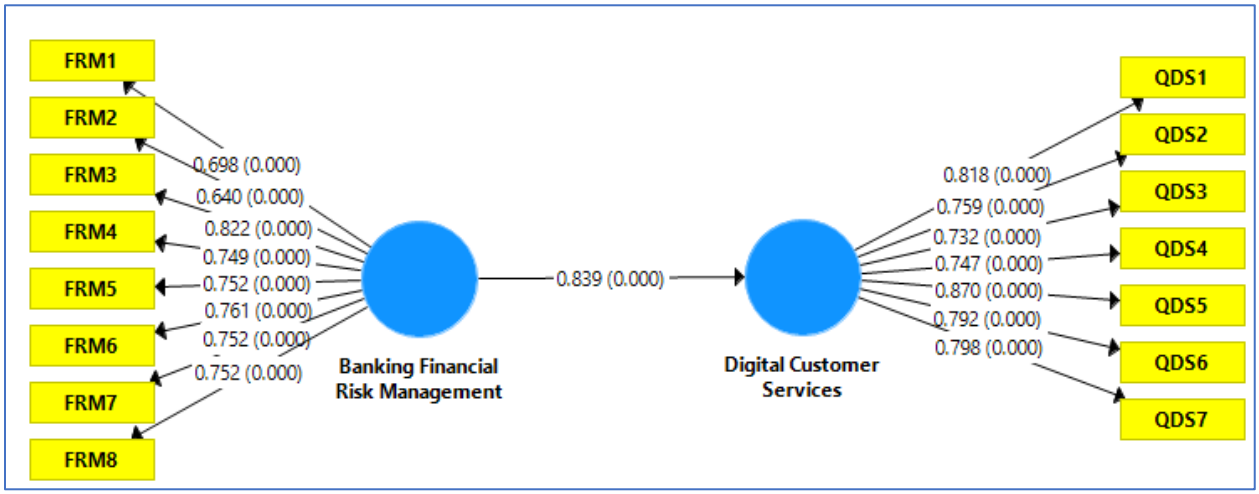

Fig 4. Regression analysis test for Banking Financial Risk Management and Digital Customer Services variable.

The results of the statistical analysis in Table (2) and Figure (4) confirm a strong and statistically significant relationship between banking financial risk management and digital customer services (regression coefficient = 0.839, p-value = 0.00), where the high values of (T=40.436) and the low standard deviation (0.021) indicate the reliability and stability of the model, confirming that improving risk management is closely related to enhancing the quality of digital services provided to customers.

2.4.2 Regression analysis test of the Banking Financial Risk Management variable and the Digital Customer Services through the moderating effect of Cybersecurity :

The table and figure present the results of a regression analysis to examine the effect of Regression analysis test of the Banking Financial Risk Management variable and the Digital Customer Services through the moderating effect of Cybersecurity .

Table 3 Regression analysis test of the Banking Financial Risk Management variable and the Digital Customer Services through the moderating effect of Cybersecurity .

Variables	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Values
Banking Financial Risk Management -> Digital Customer Services	0.505	0.507	0.056	8.944	0.00
Cybersecurity -> Digital Customer Services	0.411	0.411	0.057	7.264	0.00
Moderating Effect 1 -> Digital Customer Services	0.160	0.417	0.043	3.720	0.00

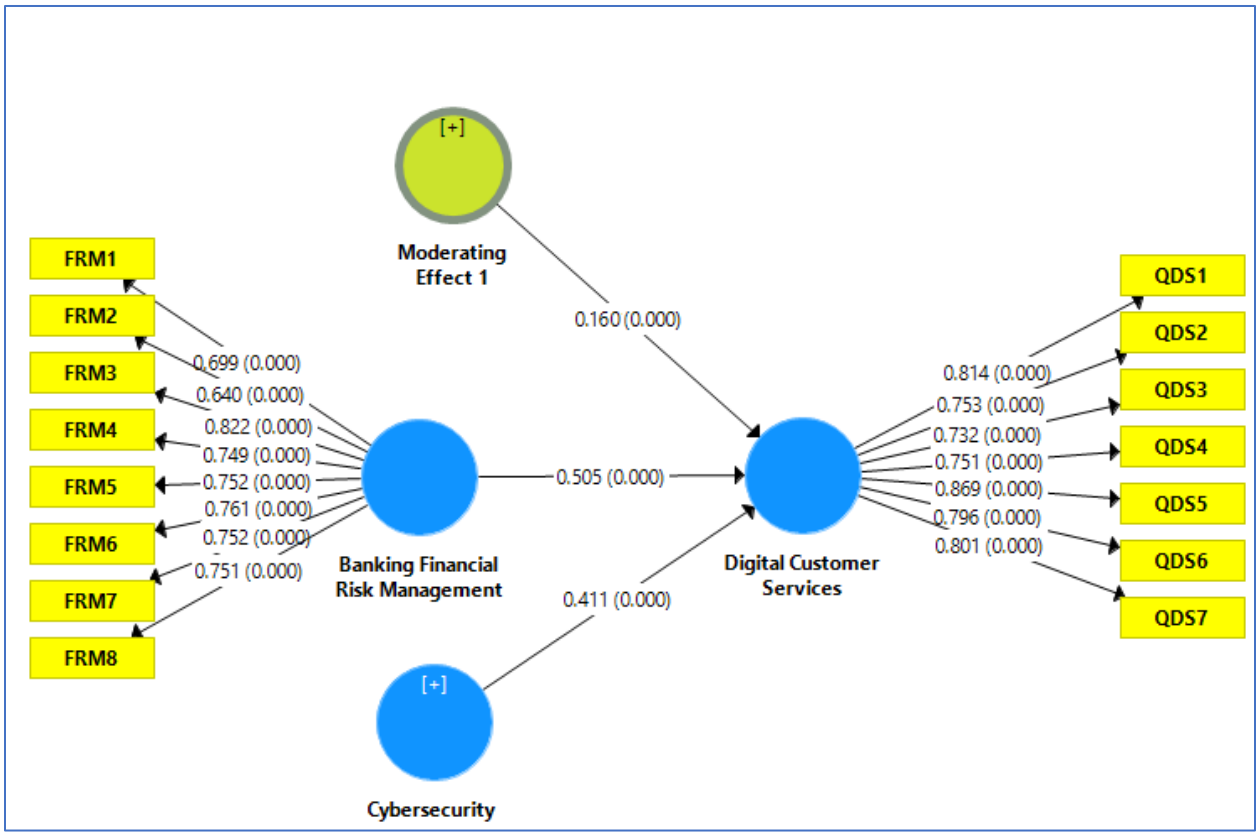

Fig 5. Regression analysis test of the Banking Financial Risk Management variable and the Digital Customer Services through the moderating effect of Cybersecurity .

The results of the multiple regression analysis in Table (3) and Figure (5) confirm:

Banking financial risk management has a strong and direct impact on digital customer services, with a regression coefficient of 0.505 ($p < 0.001$), indicating that improved risk management is associated with significant improvements in digital service quality.

As for the role of cybersecurity as a moderating factor, the recorded regression coefficient was 0.160 ($p < 0.001$), which is highly statistically significant, indicating a moderating and reinforcing effect on the relationship between banking financial risk management and digital customer services.

All results are supported by large t-values (ranging from 3.720 to 8.944) and low standard deviations (ranging from 0.043 to 0.057), confirming the reliability of the model and the consistency of its results.

CONCLUSION

The study results indicate a strong relationship between improving banking financial risk management and enhancing the quality of digital services provided to customers. The impact coefficient was 0.505, a strong indication that banks that adopt advanced risk management methods are better able to provide superior digital services. Cybersecurity also showed a clear impact of 0.411, confirming its fundamental importance in enhancing customer trust and the stability of digital systems.

The results also confirmed the role of cybersecurity as a moderating factor, with a coefficient of 0.160, as well as its high statistical significance, indicating that its impact appears to strengthen the relationship between risk management and digital services. All results were statistically consistent, with high t-values ranging from 3.720 to 8.944, and low standard deviations, enhancing the credibility of the proposed model.

These results highlight the need to adopt an integrated strategy that combines enhancing financial risk management and improving cybersecurity, as both factors contribute independently and cumulatively to improving the digital customer experience. This also underscores the importance of continuing to invest in security infrastructure and

modern risk management technologies, not only as a preventative measure but also as a key competitive factor in attracting and retaining customers in the growing digital banking market.

REFERENCES

1. Al Zubaidi, H. H. A., Fenjan, A. Z., Rageeb, A. W. N., Fayez, A. S., & Yasir, M. H. The Impact of Financial Intelligence on Banking Performance-An Analytical Study of a Sample of Commercial Banks for the Period from 2013 to 2022.
2. Annarelli, A., & Palombi, G. (2021). Digitalization capabilities for sustainable cyber resilience: a conceptual framework. *Sustainability*, *13*(23), 13065.
3. Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming!. *Comparative Strategy*, *12*(2), 141-165.
4. Bankuoru Egala, S., Boateng, D., & Aboagye Mensah, S. (2021). To leave or retain? An interplay between quality digital banking services and customer satisfaction. *International journal of bank marketing*, *39*(7), 1420-1445.
5. Bapat, D. (2022). Exploring the relationship between lifestyle, digital financial element and digital financial services experience. *International Journal of Bank Marketing*, *40*(2), 297-320.
6. Bessis, J. (2011). *Risk management in banking*. John Wiley & Sons.
7. Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. In *New Contributions in Information Systems and Technologies: Volume 1* (pp. 311-316). Cham: Springer International Publishing.
8. Bodeau, D. J., Graubart, R., Picciotto, J., & McQuaid, R. (2011). Cyber resiliency engineering framework.
9. Colye, B,(2000), Measuring credit risk , CIB publishing United Kingdom .
10. Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, *5*(1), tyz013.
11. ESRB (2020), The General Board of the European Systemic Risk Board held its 36th regular meeting on 19 December 2019, Press Release, retrieved from https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200107~29129d5701.en.html.
12. Fischer,E,(2016)Cybersecurity issues and challenges: in brief, Senior Specialist in Science and Technology, Congressional Research Service.
13. Greenberg, A. (2020). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Anchor.
14. Huang, J., Liu, F., & Zhang, J. (2024). Multi-dimensional QoS evaluation and optimization of mobile edge computing for IoT: A survey. *Chinese Journal of Electronics*, *33*(4), 859-874.
15. Kochovski, P., Drobintsev, P. D., & Stankovski, V. (2019). Formal quality of service assurances, ranking and verification of cloud deployment options with a probabilistic model checking method. *Information and Software Technology*, *109*, 14-25.
16. Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., & Seager, T. P. (2013). Measurable resilience for actionable policy.
17. Luo, D., Luo, M., & Lv, J. (2022). Can digital finance contribute to the promotion of financial sustainability? A financial efficiency perspective. Sustainability, 14(7), 3979.
18. Madueke, C. J., & Eyupoglu, S. (2024). Sustaining Economic Growth: E-Service Quality's Role in Fostering Customer Loyalty in Nigeria SMEs. *Sustainability*, *16*(21), 9175.
19. Manab, N. A., Kassim, I., & Hussin, M. R. (2010). Enterprise-wide risk management (EWRM) practices: Between corporate governance compliance and value. *International Review of Business Research Papers*, *6*(2), 239-252.
20. Nanda,A.(2024) Risk Management in Banks–Beyond Regulations, The Journal of Indian Institute of Banking & Finance, https://www.iibf.org.
21. Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa istanbul review*, *18*(4), 329-340.
22. Petrenko, S. (2022). Cybersecurity . River Publishers.
23. Rampini, A,A. Viswanathan, S. Vuillemey, G.(2016) Risk Management in Financial Institutions, J.E.L. Codes: G21, G32, D92, E44.
24. Rid, T. (2012). Cyber war will not take place. Journal of strategic studies, 35(1), 5-32.
25. Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. Journal of strategic studies, 38(1-2), 4-37.
26. Ritchie, R. (2019). Maersk: Springing back from a catastrophic cyber-attack. I–Global Intelligence for Digital Leaders.

27. Sharma, H., & Díaz Andrade, A. (2023). Digital financial services and human development: current landscape and research prospects. Information Technology for Development, 29(4), 582-606.
28. Sithipolvanichgul, J., (2016), "Enterprise Risk Management and Firm Performance: Developing Risk Management Measurement in Accounting Practice", Doctor of Philosophy The University of Edinburgh.
29. Stulz,R.M.(2016) Risk Management, Governance, Culture, and Risk Taking in Banks, FRBNY Economic Policy Review.
30. Vo, N. T., Chovancová, M., & Tri, H. T. (2020). The impact of E-service quality on the customer satisfaction and consumer engagement behaviors toward luxury hotels. *Journal of quality assurance in hospitality & tourism*, *21*(5), 499-523.
31. Yadav, D. (2023). A Framework for Implementing Data Integrity Program Enabling Mid-Size Financial Institutions to Meet United States Federal Reserve Data Quality Requirements for Model Risk Management (Doctoral dissertation, University of Arkansas at Little Rock).