

Cybersecurity and Customer Satisfaction in Digital Banking: Evidence from Nigeria

Victor Oluwatosin Ologun^{a*}, Isaac Yusuf^b, Chiamaka Beauty Obioha^c, Jamiu Olamilekan Akande^d, Abdulrazaq Ameen^e, Stephen Alaba John^f

^aDepartment of Information System, Le Moyne College Syracuse, New York, USA

^bDepartment of Mathematics, University of Ibadan, Nigeria

^cDepartment of Accounting, Crawford University, Ogun State, Nigeria

^dCentre for Cyberspace Studies, Nasarawa State University. Keffi, Nigeria

^eDepartment of Engineering and Computing, University of East London. United Kingdom

^fDepartment of Accounting and Finance, Kwara State University, Malete, Nigeria

Received 7 July 2025; Revised 28 September 2025; Accepted 24 October 2025

ABSTRACT

In the rapidly evolving digital banking environment, cybersecurity has emerged as a critical factor influencing customer trust, system usage, and overall satisfaction. However, the emergence of cybersecurity has been accompanied by a parallel rise in cyberthreats, including data breaches, online fraud, phishing attacks, and other forms of cybercrime. This study integrates a cybersecurity system into the Information Systems Success Model (ISSM) to examine its effects on customer satisfaction as Nigeria's banking industry undergoes digital transformation. Using a quantitative research approach, data were collected through structured questionnaires administered to 315 respondents, including bank customers, employees, and IT managers. An Ordered Logistic Regression (OLR) model was employed to test the predictive power of each explanatory variable. The findings show that information quality, service delivery, system use, and user satisfaction are critical drivers of customer satisfaction in digital banking. In contrast, system quality and net benefits are less influential, suggesting that trust and perceived value matter more than technical specifications alone. Strengthening user trust through secure systems and effective support will enhance satisfaction and loyalty in the digital banking environment. By integrating cybersecurity into the ISSM framework, this study offers fresh insights into technology-customer dynamics in emerging markets like Nigeria, highlighting the human-centered aspects of cybersecurity that shape satisfaction beyond technical efficiency.

KEYWORDS

Cybersecurity
Customer Satisfaction
Customer Trust
Information Systems Success Model
Digital Banking

INTRODUCTION

The global banking ecosystem has undergone a profound shift toward digitization, characterized by online transactions, mobile banking, and the adoption of emerging technologies such as blockchain

*Corresponding Author: ologunv@gmail.com; doi: 10.35313/ijabr.v8i01.579

and artificial intelligence. These innovations have not only improved accessibility and convenience but also intensified competition among banks, compelling them to invest heavily in digital infrastructure (Lottu et al., 2023; Ionaşcu et al., 2023; Chahal, 2023; Darwish, 2023). In a time when digital technologies are evolving at a breakneck pace, the banking sector is leading the way in revolutionary transformation, using new technology to improve services in an increasingly interconnected world, reach more customers, and operate more efficiently across the globe, including Nigeria (Nwakpa, 2023; Osita et al., 2023).

While the advancements offer unprecedented convenience, efficiency, and customer satisfaction, they also introduce new vectors for cyber threats, ranging from malicious actors seeking unauthorized access to financial data to the potential disruption of critical banking infrastructure, thereby undermining customer trust and threatening the stability of financial institutions (George, 2023; Mishra, 2023; Srinadi et al., 2023). Cybersecurity continues to evolve in response to emerging threats from hackers and other cybercriminals (Alqudhaibi et al., 2023). Cram et al. (2023) noted that the primary objectives of cybersecurity are to ensure the continuous operation of banking systems, protect sensitive data, and maintain information integrity. Lee (2021) affirmed that access to sensitive data should be restricted to authorized individuals. The need to protect sensitive data, prevent cyberattacks, and ensure that digital systems remain secure and resilient has become critical for banks worldwide as they strive to balance innovation, security, and customer satisfaction (Ducastel et al., 2023; Wanof, 2023). Individuals, businesses, governments, and cybersecurity professionals must work collaboratively to create a secure and resilient digital environment (Tariq et al., 2024; Wang et al., 2022).

Customer satisfaction in this digital age hinges not only on the quality of banking services but also on the perceived safety and reliability of the digital platforms. As banking systems become increasingly complex, customers are growing more concerned about the confidentiality, integrity, and availability of their financial information (Nilashi et al., 2023; Cui et al., 2023). Li and Liu (2021) noted that cybersecurity concerns are largely driven by the need to ensure safety and protect personal information. Consequently, cybersecurity has evolved from a purely technical concern into a core component of customer experience and satisfaction (Shah et al., 2023).

However, digital transformation has opened new avenues for cybercriminals who often aim at compromising the confidentiality, integrity, or availability of information systems and data. Numerous customers have reported cases of unauthorized transactions, phishing scams, and identity theft, leading to a decline in trust in online banking platforms. Cyber threats originate from diverse sources, including external hackers and internal actors, and manifest in various forms such as supply chain attacks, malware, and social engineering. Common threats include ransomware, phishing, and malware (Meduri, 2024; Mijwil et al., 2023).

Banks use prevention methods to reduce these risks (Cross, 2022; Abdulrahman, 2019). Meduri (2024) identified key vulnerabilities, including human error, inadequate network security, outdated software, and weak authentication mechanisms. Addressing these vulnerabilities requires robust security measures such as regular security audits, encryption, multi-factor authentication, and intrusion detection systems. Progressive banks can outperform competitors and improve customer satisfaction by being resilient, having a clear strategy, and focusing on customer needs (Chakraborty et al., 2023; de Azambuja et al., 2023).

Innovation and growth drive the Nigerian banking sector, but the need to keep up with new technologies creates challenges (Abdurrahman et al., 2023; Onyegbula et al., 2023; Maduka et al., 2023). These challenges oftentimes involve credit-related fraud, such as credit card or insurance fraud, which may cause financial losses, reputational damage, and reduced customer trust and satisfaction (Roszkowska, 2021). Hence, as financial services become more digitally integrated, the

specter of cyberthreats looms large, compelling banks to fortify their defenses against a growing, sophisticated threat landscape (Al-Smadi, 2023).

Within the African continent, Nigeria emerges as a key player in the banking sector, marked by a dynamic economy and burgeoning digital financial system (Iheanachor et al., 2023; Olaniyi et al., 2023). The Nigerian banking industry is not immune to the challenges posed by cyberthreats and has therefore implemented context-specific cybersecurity practices to address the evolving risk landscape (Zidan et al., 2023; Ogwo-Ude, 2023; Ibegbulam et al., 2023; Adebukola et al., 2023). Globally, cybersecurity in the banking sector has received increasing scholarly attention (Tariq et al., 2024; Khashman, 2023; Alkhateeb et al., 2023; Mian & Alatawi, 2023). However, existing studies, such as Hassan et al. (2024), Garba et al. (2023), and Nwankwo et al. (2023), have largely focused on cybersecurity practices, fraud prevention techniques, data availability, data confidentiality, data integrity, cybersecurity awareness, cybersecurity policy, cybersecurity education, and the technical or regulatory aspects of cybercrime mitigation.

A key limitation of prior research lies in its insufficient integration of customer-centric variables, particularly regarding how cybersecurity dimensions directly influence customer satisfaction. Specifically, previous studies have not adequately incorporated system reliability, data protection, and perceived net benefits into their analyses. Instead, cybersecurity has often been examined as an isolated organizational or compliance issue, with limited attention to its implications for customer experience, trust, and satisfaction, with the exception of Garba et al. (2023), which also considered cybersecurity awareness.

This present study, therefore, employs DeLone and McLean's Information Systems Success Model (ISSM) to move beyond a purely technical perspective of cybersecurity and focuses on the customer's perception of cybersecurity effectiveness and its influence on loyalty, trust, and continued use of digital banking platforms. This approach addresses a critical gap in the literature and offers practical insights for banks aiming to align their cybersecurity strategies with evolving customer expectations in Nigeria's increasingly digitized financial ecosystem. In other words, this study aims to examine how cybersecurity systems shape customer satisfaction within Nigeria's digital banking sector, using the ISSM as the theoretical framework.

LITERATURE REVIEW

Cybersecurity is a multidisciplinary field encompassing areas such as computer science, cryptography, information security, risk management, and human behaviour (Li et al., 2022; Eaton et al., 2019). It involves the application of different methods, tools, and regulatory frameworks to prevent, detect, and mitigate threats in the digital environment. Cybersecurity draws on theoretical foundations such as the CIA Triad, system vulnerabilities, and defense mechanisms to explain cyber threats and strategies for protecting data from malicious actors (Shah et al., 2023). More broadly, cybersecurity refers to the protection of data, computer systems, and networks from hacking, damage, or unauthorized access. It is also commonly referred to as information security or computer security (Shaikh & Siponen, 2023; Cram et al., 2023).

Cybersecurity is a complex and continuous process that requires collaboration, ongoing learning, and proactive action to safeguard digital environments from evolving threats and attacks (Lee, 2021). It employs policies, strategies, and technological solutions to prevent the misuse of electronic information and systems, ensure their uninterrupted operation, and protect the privacy and security of personal data. As financial activities increasingly migrate to digital platforms, banks are now at the forefront of fighting cyberattacks. While technology brings innovation, it also creates new and

complex cyber risks for financial institutions. Customers now benefit from enhanced services such as real-time transactions, mobile applications, and online banking. Consequently, banks place greater emphasis on cybersecurity to protect sensitive information, maintain customer trust, and ensure that digital systems operate securely and reliably (Kumar & Mallipeddi, 2022; Janvrin & Wang, 2022).

Customer satisfaction refers to the psychological state resulting from a customer's evaluation of a product or service based on the extent to which it meets or exceeds expectations (Nilashi et al., 2023). Ayman et al. (2022) explained customer satisfaction as an indicator of the degree to which customers are pleased with an organization's offerings. It reflects the discrepancy between expected and perceived performance. In the banking industry, as in other service sectors, customer satisfaction plays a critical role in shaping organizational performance and competitiveness (Cui et al., 2023).

Commercial banks consistently seek to enhance customer satisfaction by improving the quality of their products and services (Jadon, 2022). Failure to deliver reliable and high-quality services may prompt customers to switch to competing banks. Sustaining competitive advantage in the financial market depends largely on the ability to deliver superior service that meets customer expectations. Given the highly competitive nature of the financial sector, banks are increasingly adopting customer-oriented strategies to better understand consumer preferences and strengthen their competitive positioning (Tiwari, 2022; Karimov & Jasurovich, 2022). When banks effectively satisfy customer needs, they are more likely to achieve higher profitability, operational efficiency, and customer retention. Accordingly, the provision of high-quality service remains a critical determinant of banks' long-term performance and competitiveness (Klimontowicz & Majewska, 2022; Sugiarto & Octaviana, 2021).

Theoretical Review

This study is anchored in the Information Systems Success Model (ISSM), originally proposed by William DeLone and Ephraim McLean in 1992 and revised in 2003. The model provides a comprehensive framework for assessing the success of information systems (IS). The ISSM comprises six interrelated dimensions: information quality, system quality, service quality, use, user satisfaction, and net benefits. Each dimension contributes to understanding how information systems deliver value to organizations and their stakeholders. Cybersecurity significantly impacts each dimension of the ISSM, ultimately influencing customer satisfaction in the banking sector. Specifically, robust cybersecurity measures ensure that data managed and processed by banking information systems are accurate, reliable, and protected from unauthorized access and breaches. Customers value accurate and secure information, which leads to higher trust and confidence in the bank's ability to safeguard personal and financial data.

A secure banking system is characterized by high reliability and uptime, with minimal disruptions caused by cyber threats. Effective cybersecurity measures contribute to system stability and performance. Reliable and consistently available banking services ensure a positive user experience, thereby reducing frustration and increasing customer satisfaction. In addition, high-quality cybersecurity services include prompt and effective responses to security incidents, comprehensive user training, and clear communication about security protocols. When customers feel supported and well-informed about security measures, their overall satisfaction with the bank's services improves. Furthermore, enhanced cybersecurity increases user confidence in the banking system, encouraging more frequent and diverse use of digital banking services. Greater utilization of secure and convenient digital banking services contributes to higher customer satisfaction due to

the ease and flexibility these platforms provide. User satisfaction is therefore directly influenced by customers' perceptions of the security and reliability of the banking system. Effective cybersecurity measures reduce the risk of data breaches and fraud, contributing to a sense of security and trust. Users who perceive banking systems as secure are more likely to report positive banking experiences, resulting in greater loyalty and favorable word-of-mouth.

Overall, by protecting banks and customers from reputational damage and financial losses due to cyber incidents, cybersecurity delivers significant net benefits. These benefits include improved operational efficiency, reduced fraud, and enhanced customer trust. The net benefits realized through strong cybersecurity measures contribute to the overall success of banks, ultimately translating into higher levels of customer satisfaction and retention.

Empirical Review

Ayman et al. (2022) examined the key factors influencing customer satisfaction in Jordan's banking industry and assessed the impact of technology adoption on customer satisfaction. The results showed that customer satisfaction with the quality of e-services is a key factor for e-banking success. To meet customer expectations and improve satisfaction, e-banks need to provide good-quality, available, accessible, and interactive services. They must also continuously adapt to rapid technological advancements.

Al-Araj et al. (2022) investigated the application of artificial intelligence (AI) in the banking sector using exploratory factor analysis and found that the updated SERVQUAL model comprises five dimensions instead of the original eight: tangibility, assurance, reliability, responsiveness, and empathy. The study demonstrated that AI plays a significant role in enhancing service quality and customer satisfaction. The revised model provided a more refined framework for understanding customer satisfaction in banking. The findings suggested that AI is highly relevant to customers in Jordan's banking sector and that an appropriate balance between virtual and human agents should be maintained based on customer preferences. The study also identified practical implications of AI for shaping customers' perceptions of banking services.

Khashman (2023) examined the determinants of customer satisfaction in Jordan's banking industry. Using quantitative techniques, the study found that customer satisfaction increases significantly when banks employ skilled staff and provide assurance, responsiveness, advanced technology, security, and privacy. The findings also emphasized that delivering error-free services is critical for enhancing customer satisfaction and loyalty.

Alkhateeb et al. (2023) examined the factors influencing customer satisfaction in Kuwait's banking sector through the analysis of focus group interviews. The study revealed that higher levels of customer satisfaction contribute to increased customer loyalty and retention. Satisfied customers are also more likely to recommend the bank to friends and family. Customer satisfaction was found to depend on factors such as professional staff conduct, transparency in transaction handling, and effective customer support, all of which contribute to building trust in banking institutions.

Mian and Alatawi (2023) used Smart PLS to study the effects of perceived usefulness, technical readiness, training, and user satisfaction affect cybersecurity adoption. The findings indicated that user satisfaction is strongly influenced by perceived usefulness, training, and technical readiness. Also, higher levels of user satisfaction increase the likelihood of cybersecurity adoption. The study also highlighted the mediating role of user intention in this relationship.

Choudhary et al. (2023) applied descriptive statistical techniques to examine the impact of FinTech adoption on customer satisfaction in the banking sector. The results showed that FinTech has become an integral component of the financial industry and significantly enhances customer

satisfaction. The study further suggested that customers readily accept and adapt to emerging financial technologies.

Garba, Kaur, and Ibrahim (2023) examined human-related factors influencing cybersecurity culture among Nigerian online banking customers. Their findings highlighted the importance of cybersecurity education, policy, and awareness in fostering a security-oriented mindset. Among these factors, cybersecurity awareness emerged as the most influential, followed by cybersecurity policy and education, in promoting security-conscious behavior among customers.

Oyewole et al. (2024) reviewed past research and recent cybersecurity cases to assess the current state of cybersecurity, evaluate existing frameworks, and suggest ways to improve digital protection. The findings indicated that banks must adopt adaptive cybersecurity strategies that include advanced technologies, regulatory compliance, and build a security-aware culture. The study concluded that banks need a complete and adaptable approach to cybersecurity, supported by smart investments in technology, training, and teamwork.

Hassan et al. (2024) investigated cybersecurity in Nigeria's banking industry by looking at how banks respond to incidents, follow rules, and work with global cybersecurity groups. Using case study methods, the study found that banks must continuously adapt, cooperate, and innovate to safeguard banking systems amid the ongoing evolution of digital finance, both within Nigeria and globally.

RESEARCH METHOD

This study utilized primary data obtained through structured questionnaires distributed to customers, employees, and IT managers of five (5) deposit money banks in Nigeria. The sampled banks included Zenith Bank, First Bank, Guaranty Trust Bank, Access Bank, and United Bank for Africa (UBA). This study used a survey research design. The research instrument comprised two sections. Part A gathered respondents' personal information, while Part B contained items measured using a five-point Likert scale ranging from strongly agree (5 points) to strongly disagree (1 point). In the demographic analysis, the questionnaire provided a distribution of respondents by gender, age group, responder category, and educational level. Subsequently, the reliability of measurement scales adapted from the literature was assessed using the reliability coefficient indicator, alongside multiple items designed to evaluate service quality and customer satisfaction.

A total of 315 questionnaires were distributed, and 168 were completed and returned, yielding a usable response rate of 53.33%. The relatively low response rate could be attributed to limited literacy levels among some bank customers. Given that the study involved technical constructs related to cybersecurity, such as system quality, data protection, and net benefits, respondents with lower educational attainment or limited digital literacy may have found the questionnaire difficult to comprehend or intimidating. This may have resulted in non-completion or refusal to participate, particularly among individuals who lacked confidence in interpreting or responding accurately to the survey items. Furthermore, in regions where digital banking adoption remains uneven, customer awareness and familiarity with cybersecurity concepts may be limited, further constraining survey participation.

The constructs used in this study were adapted from established scales in the information systems and cybersecurity literature to ensure content validity. Expert reviews conducted by academics in information systems and banking professionals were used to refine item wording and ensure contextual relevance to Nigeria's digital banking environment. Construct validity was confirmed through internal consistency reliability testing, with Cronbach's Alpha values ranging

from 0.76 to 0.88, indicating acceptable to excellent reliability. To minimize common method bias, questionnaire items were randomly ordered, and respondents were assured of anonymity to reduce social desirability bias. Participation was voluntary, and informed consent was obtained from all respondents. Confidentiality of responses was maintained, and no personally identifiable information was collected. Ethical approval was obtained from the University Research Ethics Committee, Kwara State University, Nigeria, to ensure compliance with standard research ethics.

Model Specification

A simple Ordered Logistic Regression (OLR) model was specified for this study as follows:

$$CSA = f(IFQ, SYQ, SEQ, USE, SAT, NBE) \quad (1)$$

Where: CSA represents customer satisfaction; IFQ represents information quality; SYQ represents system quality; SEQ represents service quality; USE represents use; SAT represents user satisfaction; and NBE represents net benefits.

To further explore how these variables affect customer satisfaction, the OLR functional model was specified:

$$\text{logit}(P(Y \leq z | X)) = \alpha_z - \beta_1 IFQ_1 - \beta_2 SYQ_2 - \beta_3 SEQ_3 - \beta_4 USE_4 - \beta_5 SAT_5 - \beta_6 NBE_6$$

Where: z represents the z -th threshold (cut-point) of the dependent variable, with $= 1, 2, \dots, K-1$; α_z is a vector of logit coefficients thresholds to be estimated; $\beta_1, \beta_2, \beta_3, \beta_4, \beta_5$, and β_6 are the coefficients of the independent variables.

Hence, the logit function $\text{logit}(P(Y \leq z | X))$ represents the natural logarithm of the odds that the dependent variable Y is less than or equal to category j . The cut-points α_z determine the boundaries between the ordered categories of the dependent variable.

OLR is appropriate for this study because it is specifically designed for dependent variables with naturally ordered categories. Also, it can accommodate skewed and non-normal data distributions better than linear regression, which assumes normally distributed residuals.

Table 1: Distribution of respondents

Constructs	Items	Frequency	Percentage (%)
Gender	Male	97	57.74
	Female	71	42.26
Age Group	20-29 years"	44	26.19
	30-39 years"	43	25.60
	40-49 years"	48	28.57
	50 and above"	33	19.64
Respondent category	Employees	50	29.76
	IT Managers	10	6.00
	Customers	108	64.29
Highest Qualification	Graduate studies	51	30.36
	Bachelor	54	32.14
	Diploma	40	23.81

Constructs	Items	Frequency	Percentage (%)
	High School	23	13.69
Total		168	100%

Source: Authors Own Work

The distribution of respondents in the study reflects a diverse and relevant sample for examining cybersecurity and customer satisfaction in Nigeria's banking sector. Out of the total 168 respondents, 97 (57.74%) were male, and 71 (42.26%) were female, indicating a slightly male-dominated sample. In terms of age, the largest group of respondents fell within the 40–49-year age bracket (28.57%), followed by those aged 20–29 years (26.19%) and 30–39 years (25.60%), while the smallest group comprised respondents aged 50 and above (19.64%). This distribution suggests that most participants are within the economically active and digitally engaged age range.

Regarding respondent categories, the majority (64.29%) were bank customers, 29.76% were bank employees, and 6.00% were IT managers. This distribution ensures that the study captures perspectives from both end users and institutional actors involved in digital banking services. The educational qualifications of the respondents further indicate a relatively well-informed sample, with 32.14% holding a bachelor's degree, 30.36% having graduate-level education, 23.81% holding diplomas, and 13.69% having only a high school qualification. This indicates that most participants have sufficient educational background to understand and provide informed opinions on cybersecurity issues and customer satisfaction. Overall, the demographic and professional diversity of the sample enhances the validity and analytical depth of the study's findings.

RESULTS

Reliability of Variables

To ensure the robustness of the measurement model, the internal consistency method was employed to assess the reliability of the study variables. Internal consistency examines the extent to which multiple items measure the same construct. Cronbach's alpha is a widely used indicator for evaluating internal consistency reliability. Higher Cronbach's alpha values indicate stronger reliability, typically ranging from 0.60 to 0.90. Values between 0.70 and 0.90 are generally considered good, while values between 0.60 and 0.70 are deemed acceptable (Hair et al., 2022).

Table 2. Internal consistency reliability

Construct	No. of Items	Cronbach's Alpha	Interpretation
Customer Satisfaction (CSA)	4	0.861	Excellent reliability
Information Quality (IFQ)	4	0.844	Good reliability
System Quality (SYQ)	4	0.798	Acceptable reliability
Service Quality (SEQ)	3	0.813	Good reliability
Use (USE)	3	0.762	Acceptable reliability
User Satisfaction (SAT)	4	0.880	Excellent reliability
Net Benefits (NBE)	4	0.835	Good reliability

Source: Authors Own Work

All constructs have a Cronbach's Alpha ≥ 0.76 , indicating that the items used to measure each construct are reliable and internally consistent. The overall Cronbach's Alpha of 0.880 shows that the full scale used in the questionnaire is highly reliable for analyzing how cybersecurity systems influence customer satisfaction in Nigeria's banking industry.

Normality Test

A normality test was conducted to check if a dataset follows a normal (Gaussian) distribution. In such a distribution, the mean, median, and mode coincide and are located at the center of a symmetrical, bell-shaped curve.

Table 3. Normality test results

H₀: "Data were drawn from a normally distributed population."

Shapiro-Wilk Statistic	Df	Sig.
0.968	68	0.2073

Source: Authors Own Work

The Shapiro-Wilk test and model p-values were used to check if the data are normally distributed. The model's p-value is 0.2073, and the Shapiro-Wilk statistic is 0.968. Since the p-value exceeds 0.05, there is insufficient evidence to reject the null hypothesis of normality. Therefore, the data are considered to be normally distributed.

Table 4: Chi-Square results

Chi-Square test was conducted to examine the link between cybersecurity and customer satisfaction.

Statistic	Value
Pearson Chi-square	14.5532
Degrees of Freedom (df)	4
Asymptotic Sig. (p)	0.0000
Interpretation	Since $p < 0.05$, there is a statistically significant association between cybersecurity and customer satisfaction.

Source: Authors Own Work

With the p-value below 5%, the null hypothesis is rejected. This finding suggests that customers' perceptions of cybersecurity system effectiveness significantly affect their level of satisfaction. As such, strong cybersecurity measures may enhance customer trust and satisfaction, while weak cybersecurity may adversely affect customer satisfaction.

Ordered Logistic Regression (OLR)

Ordered Logistic Regression (OLR) is a suitable and robust method for analyzing data collected from primary sources. It provides consistent and reliable estimates, even with relatively small sample sizes. This is because OLR does not require the dependent variable to be normally distributed and performs well when the data are ordinal in nature or deviate from normality, making it appropriate for survey-based research.

Table 5. Ordered logistic regression estimates

Dependent Variable: Customer Satisfaction			
Variables	Coefficients	Odds ratio	Probs.
IFQ	0.01908	1.9262	0.0000
SYQ	-0.17813	0.7829	0.1113
SEQ	0.04785	1.8823	0.0000
USE	0.04676	1.1791	0.0000
SAT	0.20510	1.2270	0.0000
NBE	0.12532	1.1335	0.0000
P-LR Chi-Square	0.00043		
Pseudo R-Square	0.76425		

Source: Authors Own Work

DISCUSSION

Information Quality (IFQ: $\beta = 0.01908$, OR = 1.9262, $p < 0.05$)

The positive and statistically significant coefficient indicates that higher information quality substantially increases the likelihood of customers reporting higher satisfaction levels. The odds ratio of 1.93 suggests that for every one-unit increase in information quality, the odds of moving into a higher satisfaction category nearly double. This indicates that improvements in information quality, such as accuracy, reliability, and data security, are associated with higher customer satisfaction. When banks provide accurate, secure, and trustworthy information through digital banking platforms and clear communication channels, customer confidence and satisfaction improve. These findings align with the ISSM dimension of information quality, which emphasizes accuracy, reliability, and security of information. In the banking context, customers value timely and trustworthy financial data, clear communication, and well-protected information, all of which enhance satisfaction and trust in the institution.

System Quality (SYQ: $\beta = -0.17813$, OR = 0.7829, $p > 0.05$)

The negative coefficient indicates that higher system quality is associated with a slight reduction in the odds of customers reporting greater satisfaction; however, this effect is statistically insignificant ($p > 0.05$). The odds ratio of 0.78 implies that a one-unit increase in perceived system quality corresponds to a 22% reduction in the odds of moving to a higher satisfaction level. Despite the negative sign, the lack of statistical significance suggests that system quality does not exert a meaningful influence on customer satisfaction in this study. This suggests that poor system quality could lead to lower customer satisfaction. While ISSM highlights system quality as critical to system success, this finding suggests it is less influential compared to other dimensions. Customers may tolerate technical shortcomings (e.g., occasional downtime or slow performance) as long as information and service quality remain strong. This reflects a context-specific dynamic in Nigeria's banking sector, where customers prioritize security, communication, and usability over purely technical system performance.

Service Quality (SEQ: $\beta = 0.04785$, OR = 1.8823, $p < 0.05$)

Service quality demonstrates a strong, positive, and significant effect on customer satisfaction. The odds ratio of 1.88 indicates that each unit increase in service quality nearly doubles the likelihood of higher customer satisfaction. This finding confirms that responsive customer support and well-managed services are central drivers of satisfaction in digital banking environments. As the digital banking service quality improves (through clearer communication, faster response times, and effective problem resolution), customer satisfaction correspondingly increases. This finding reinforces the ISSM service quality dimension, which emphasizes responsiveness and effective communication. High-quality cybersecurity-related services, including timely incident response, customer education on security practices, and accessible support channels, directly enhance customer satisfaction, underscoring the importance of service delivery in digital banking success.

Use (USE: $\beta = 0.04676$, OR = 1.1791, $p < 0.05$)

The positive and significant relationship indicates that increased usage of digital platforms is associated with higher satisfaction. The odds ratio of 1.18 implies that more frequent use increases the likelihood of customers reporting higher satisfaction by approximately 18%. This suggests that customers who regularly engage with digital banking services, such as online banking platforms and mobile applications, tend to report greater satisfaction with their banking experience. Frequent interaction with secure and user-friendly digital platforms reinforces convenience, confidence, and perceived value, thereby enhancing satisfaction. Thus, increasing customer engagement with user-friendly, accessible, and secure digital services is an effective strategy for improving customer satisfaction. This finding reflects the ISSM use dimension, which captures the extent and effectiveness of system utilization. Secure, user-friendly platforms encourage customers to adopt digital banking services more often, and frequent engagement strengthens satisfaction by offering convenience, flexibility, and confidence in the system.

User Satisfaction (SAT: $\beta = 0.20510$, OR = 1.2270, $p < 0.05$)

User satisfaction with specific banking services exerts a significant and positive effect on overall satisfaction. With an odds ratio of 1.23, a one-unit increase in user satisfaction raises the odds of higher overall satisfaction by 23%. This implies that user satisfaction with specific banking services (e.g., platform usability, transaction security, and customer support experience) contributes significantly to customers' overall evaluation of the bank. Positive individual service experiences translate into broader satisfaction with the institution, reinforcing the importance of consistently meeting user expectations. This finding further confirms the ISSM's idea that satisfied users contribute to broader system success and positive perceptions of service value.

Net Benefits (NBE: $\beta = 0.12532$, OR = 1.1335, $p = 0.2554$)

The positive and significant coefficient shows that greater perceived net benefits of cybersecurity systems significantly increase customer satisfaction. The odds ratio of 1.13 indicates that every one-unit rise in perceived net benefits improves the odds of a customer reporting a higher level of satisfaction by 13%. This suggests that when customers see tangible benefits, such as reduced fraud, smoother transactions, improved trust, and overall efficiency, they are more likely to feel satisfied with the bank. In other words, beyond technical features, the broader value customers associate with cybersecurity investments translates into stronger satisfaction outcomes. This finding reflects the ISSM net benefits dimension, which captures the tangible and intangible value of information systems. Customers who perceive practical benefits, such as reduced fraud, smoother transactions, enhanced trust, and efficiency, are more likely to report higher satisfaction.

The summary of the study's results is shown in Table 6.

Table 6. Summary of findings

Hypothesis	Description	Remark
H ₀₁	Information quality does not significantly affect customer satisfaction	Reject
H ₀₂	System quality does not significantly affect customer satisfaction	Accept
H ₀₃	Service quality does not significantly affect customer satisfaction	Reject
H ₀₄	Use does not significantly affect customer satisfaction	Reject
H ₀₅	User satisfaction does not significantly affect customer satisfaction	Reject
H ₀₆	Net benefit does not significantly affect customer satisfaction	Accept

Source: Authors Own Work

CONCLUSION

This study concludes that the Information Systems Success Model (ISSM) is applicable to Nigeria's banking industry, as cybersecurity systems significantly affect customer satisfaction. Therefore, the study recommends that customers actively offer feedback on their experiences with banking services, particularly regarding the effectiveness of the cybersecurity system. Bank managers should prioritize sustained investment in robust and secure cybersecurity systems, including high system uptime, reliable performance, strong resilience against cyber threats, and high-quality customer support services. In addition, policymakers should formulate and enforce comprehensive national cybersecurity strategies and robust data protection regulations to ensure that banks are held accountable for safeguarding customer data and maintaining trust in digital banking platforms.

IMPLICATIONS

First, bank managers should prioritize the delivery of accurate, reliable, and secure information, as customers place high value on the clarity, accuracy, and trustworthiness of the data they receive through online banking platforms, transaction alerts, and service updates. They should invest in strengthening information systems, enhancing communication transparency, and implementing strict data protection standards to reinforce customer trust and confidence.

Second, bank managers should focus on enhancing service delivery processes by training front-line staff, enhancing responsiveness, and providing seamless support across both digital and physical service touchpoints. High-quality service experiences, such as timely responses, courteous communication, and effective complaint resolution, reinforce customer loyalty and trust, particularly in a security-conscious digital banking environment.

Third, banks should actively promote digital adoption through intuitive user interfaces, accessible platform designs, and robust cybersecurity features. Managers should also consider implementing digital literacy campaigns or onboarding support for customers to help them feel more confident using online services. The more comfortable and engaged customers are with digital platforms, the more satisfied they tend to be with the overall banking experience.

Fourth, while system quality may not directly drive satisfaction, banks must ensure that their digital platforms are consistently functional, fast, and dependable to prevent potential negative

perceptions. This is because customers may take stable system performance for granted, but system failure or poor experience with system functionality could lead to dissatisfaction. As such, managers should treat system reliability as a baseline requirement and focus improvement efforts on areas that more directly influence satisfaction. When customers are satisfied with aspects such as mobile app usability, the security of their transactions, or the responsiveness of service channels, they are more likely to feel satisfied with the bank as a whole. Therefore, managers should continuously evaluate user feedback, conduct usability testing, and improve digital tools to ensure positive, secure, and efficient user experiences.

REFERENCES

- Abdurrahman, A., Gustomo, A., & Prasetyo, E.A. (2023). Enhancing banking performance through dynamic digital transformation capabilities and governance, risk management, and compliance: Insights from the Indonesian context. *The Electronic Journal of Information Systems in Developing Countries*, e12299.
- Adebukola, A.A., Navya, A.N., Jordan, F.J., Jenifer, N.J., & Begley, R.D. (2022). Cyber security as a threat to health care. *Journal of Technology and Systems*, 4(1), pp.32-64.
- Al-Araj, R., Haddad, H., Shehadeh, M., Hasan, E., & Nawaiseh, M.Y. (2022). The Effect of Artificial Intelligence on Service Quality and Customer Satisfaction in Jordanian Banking Sector. *WSEAS Transactions on Business and Economics*, 19, 1929-1947. DOI: 10.37394/23207.2022.19.173
- Alkhateeb, M., Almutairi, A., Alsaed, O., Alshatti, M., Alfouzan, A., & Aburumman, O.J. (2023). Factors Influencing Customers Satisfaction in Kuwait Banking Sector. *International Journal of Social Science and Humanities Research*, 11(2), 75-81. DOI: <https://doi.org/10.5281/zenodo.7846077>
- Alqudhaibi, A., Deshpande, S., Jagtap, S., & Salonitis, K. (2023). Towards a sustainable future: developing a cybersecurity framework for manufacturing. *Technological Sustainability*. <https://doi.org/10.1108/TECHS-05-2023-0022>.
- Al-Smadi, M.O. (2023). Examining the relationship between digital finance and financial inclusion: Evidence from MENA countries. *Borsa Istanbul Review*, 23(2), 464-472.
- Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
- Buil, G.D., Lord, N., & Barrett, E. (2021). The dynamics of business, cybersecurity and cyber-victimization: Foregrounding the internal guardian in prevention. *Victims & Offenders*, 16(3), 286-315.
- Chahal, S. (2023). Navigating financial evolution: business process optimization and digital transformation in the finance sector. *International Journal of Finance*, 8(5), 67-81.
- Chakraborty, A., Biswas, A., & Khan, A.K. (2023). Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In *Artificial Intelligence for Societal Issues* (pp. 3-25). Cham: Springer International Publishing.
- Choudhary, U., Dang, K., & Kaur, S. (2023). A research study on the impact of fintech on customer satisfaction in banking sector. *Journal of the Oriental Institute*, 72, 61-65.
- Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity research in accounting information systems: A review and frame work. *Journal of Emerging Technologies in Accounting*, 20(1), 15-38.
- Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging. *Crime Prevention and Community Safety*, 24(1), 30-41.
- Cui, H., Qiu, J., Cao, J., Guo, M., Chen, X., & Gorbachev, S. (2023). Route optimization in township logistics distribution considering customer satisfaction based on adaptive genetic algorithm. *Mathematics and Computers in Simulation*, 204, 28-42.
- Darem, A.A., Alhashmi, A.A., Alkhaldi, T.M., Alashjaee, A.M., Alanazi, S.M. & Ebad, S.A. (2023). Cyber

- Threats Classifications and Countermeasures in Banking and Financial Sector. *IEEE Access*, 1-21. Doi: 10.1109/ACCESS.2017.
- Darwish, D. (2023). Blockchain and Artificial Intelligence for Business Transformation Toward Sustainability. In *Blockchain and its Applications in Industry 4.0* (pp. 211-255). Singapore: Springer Nature Singapore.
- de Azambuja, A.J.G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V.R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0: A survey. *Electronics*, 12(8), 1920.
- Ducastel, A., Bourblanc, M., & Adelle, C. (2023). Why development finance institutions are reluctant to invest in agriculture... and why they keep trying. *Financializations of Development: Global Games and Local Experiments*.
- Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, 13(2), 1-9.
- Garba, J., Kaur, J., & Ibrahim, E. N. M. (2023). Design of a Conceptual Framework for Cybersecurity Culture amongst Online Banking Users in Nigeria”, *Nigerian Journal of Technology*, 42(3), 399 – 305. <https://doi.org/10.4314/njt.v42i3.13>
- George, A.S. (2023). Securing the future of finance: how ai, blockchain, and machine learning safeguard emerging neobank technology against evolving cyber threats. *Partners Universal Innovative Research Publication*, 1(1), 54-66.
- Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From Chatgpt to Threatgpt: Impact of generative AI in cybersecurity and privacy. *IEEE Access*.
- Hassan, A.O., Ewuga, S.K., Abdul, A.A., Abrahams, T.O., Oladeinde, M., & Dawodu, S.O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, 5(1), 41-59. DOI: 10.51594/csitrj.v5i.701
- Ibegbulam, M.C., Fatounde, S., & Olowonubi, J.A. (2023). Small Hydropower (SHP) development in Nigeria: an assessment, challenges, and opportunities. *International Journal of Physical Sciences Research*, 7(1), 11-35.
- Iheanachor, N., Umukoro, I., & Aránega, A.Y. (2023). Ecosystem emergence in emerging markets: Evidence from the Nigerian digital financial services ecosystem. *Technological Forecasting and Social Change*, 190, 122426.
- Ionaşcu, A.E., Gheorghiu, G., Spătaru, E.C., Munteanu, I., Grigorescu, A., & Dănilă, A. (2023). Unraveling digital transformation in banking: evidence from Romania. *Systems*, 11(11), 534.
- Jadon, R. (2022). Relationship between market orientation and service quality: with reference to Indian banks in Rajasthan. *Shod Samhita Journal*, 9(3). <https://doi.org/10.52970/grmapb.v2i1.157>
- Janvrin, D. J., & Wang, T. (2022). Linking cybersecurity and accounting: An event, impact, response framework. *Accounting Horizons*, 36(4), 67-112.
- Khashman, R.M.K. (2023). Customer Satisfaction Quality in Banking Sector. *International Journal of Business and Management*, 18(2), 15-26. <https://doi.org/10.5539/ijbm.v18n2p15>
- Klimontowicz, M., & Majewska, J. (2022). The contribution of intellectual capital to banks' competitive and financial performance: The evidence from Poland. *Journal of Entrepreneurship, Management and Innovation*, 18(2), 105-136. <https://doi.org/10.7341/20221824>
- Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, 31(12), 4488-4500.
- Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659-671.
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186.
- Li, Y., Yang, J., Zhang, Z., Wen, J., & Kumar, P. (2022). Healthcare data quality assessment for cybersecurity intelligence. *IEEE Transactions on Industrial Informatics*, 19(1), 841-848.

- Lottu, O.A., Abdul, A.A., Daraojimba, D.O., Alabi, A.M., John-Ladega, A.A., & Daraojimba, C. (2023). Digital transformation in banking: a review of Nigeria's journey to economic prosperity. *International Journal of Advanced Economics*, 5(8), 215-238.
- Maduka, C.P., Adegoke, A.A., Okongwu, C.C., Enahoro, A., Osunlaja, O., & Ajogwu, A.E. (2023). Review of laboratory diagnostics evolution in Nigeria's response to COVID 19. *International Medical Science Research Journal*, 3(1), 1-23.
- Mansour, A., Mansour, Y., Almajali, D., Majali, T., Saa'da, R.J., & Hammouri, Q. (2022). The impact of Technology adoption on Customer Satisfaction in Banking Sector in Jordan. *Journal of Positive School Psychology*, 6(6), 6200 – 6209.
- Meduri, K. (2024). Cybersecurity threats in banking: Unsupervised fraud detection analysis. *International Journal of Science and Research Archive*, 11(02), 915-925. DOI: <https://doi.org/10.30574/ijrsra.2024.11.2.0505>
- Mian, T.S., & Alatawi, E.M. (2023). Exploring Factors to Improve Intentions to Adopt Cybersecurity: A Study of Saudi Banking Sector. *Humanities and Natural Sciences Journal*
- Mijwil, M., Unogwu, O.J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the top five evolving threats in cybersecurity: an in-depth overview. *Mesopotamian Journal of Cybersecurity*, 2023, 57-63.
- Mishra, S. (2023). Exploring the impact of ai-based cyber security financial sector management. *Applied Sciences*, 13(10), 5875.
- Möller, D.P. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (231-271). Cham: Springer Nature Switzerland.
- Nilashi, M., Abumalloh, R. A., Samad, S., Alrizq, M., Alyami, S., & Alghamdi, A. (2023). Analysis of customers' satisfaction with baby products: The moderating role of brand image. *Journal of Retailing and Consumer Services*, 73, 103334.
- Nwakpa, J.N. (2023). Evaluation of Nigerian government's new cashless policy: insights from select national dailies. *British Journal of Marketing Studies*, 11(3), 1-16.
- Nwankwo, C., Kanyangale, M., Anoke, A.F., & Eze, S.U. (2023). Effect of Cyber Security on Business Sustainability of Listed Microfinance Banks in Nigeria. *Artha – Journal of Social Sciences*, 22(1), 79-106. <https://doi.org/10.12724/ajss.64.4>
- Ogwo-Ude, O. (2023). Business email compromise challenges to medium and large-scale firms in USA: An Analysis. *Open Journal of Applied Sciences*, 13(6), 803-812.
- Olaniyi, O., Olaoye, O.O., & Okunleye, O.J. (2023). Effects of Information Governance (IG) on profitability in the Nigerian banking sector. *Asian Journal of Economics, Business and Accounting*, 23(18), 22-35.
- Onyegbula, E.F., Nwoye, M.I., & Daniel, C.O. (2023). Impact of strategy implementation on the performance of regulatory and supervisory agencies in financial services sector in Nigeria. *Journal of Human Resource and Sustainability Studies*, 11(2), 298-315.
- Osita, F.C., Ozike, K.C., Okafor, N.D., & Nebolisa, C.C. (2023). Aftermath of the naira redesign on small and medium enterprises (SMEs) in Nigeria. *Journal of the Management Sciences*, 60(1), 235-244.
- Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change*, 17(2), 164-196.
- Selvaraj, N.A. (2021). The Essence of Cybersecurity Through Fintech 3.5 In Preventing and Detecting Financial Fraud: A Literature Review. *Electronic Journal of Business and Management*, 6(2), 18-29.
- Shah, I. A., Jhanjhi, N. Z., & Laraib, A. (2023). Cybersecurity and Blockchain Usage in Contemporary Business. In *Handbook of Research on Cybersecurity Issues and Challenges for Business and Fintech Applications* (pp. 49-64). IGI Global, United States.
- Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, 124, 102974.

- Srinadi, N.L.P., Hermawan, D., & Jaya, A.A.N.A. (2023). Advancement of banking and financial services employing artificial intelligence and the internet of things. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 14(1), 106-117.
- Sugiarto, S., & Octaviana, V. (2021). Service Quality (SERVQUAL) Dimensions on Customer Satisfaction: Empirical Evidence from Bank Study. *Golden Ratio of Marketing and Applied Psychology of Business*, 1(2), 93-106. <https://doi.org/10.52970/grmapb.v1i2.103>
- Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E.K., Alzboun, N., Al-Hawary, S.I.S., & Alshurideh, M.T. (2023). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. *International Journal of Data and Network Science*, 8, 1-8. doi: 10.5267/j.ijdns.2023.10.016
- Tiwari, P. (2022). Bank affection and customer retention: an empirical investigation of customer trust, satisfaction, loyalty. *SN Business & Economics*, 2, 54. <https://doi.org/10.1007/s43546-022-00229-y>
- 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.
- Wanof, M.I. (2023). Digital technology innovation in improving financial access for low-income communities. *Technology and Society Perspectives (TACIT)*, 1(1), 26-34.
- Zidan, F., Nugroho, D., & Putra, B.A. (2023). Securing enterprises: harnessing blockchain technology against cybercrime threats. *International Journal of Cyber and IT Service Management*, 3(2), 167-172.