DS Journal of Cyber Security
Volume 3 Issue 3, 39-50, Jul - Sep 2025
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V3I3P103

Original Article

Effect of Cyber Security on Organization Network: A Case Study of Selected Commercial Banks in Nigeria

Abba, Monday Okoroma[1], Osodeke, Efe Charles[2], Ibekwe, Christopher Chimaobi[3*]

[1]*Department of Information Systems and Technology, Faculty of Computing, Umuahia Study Centre, National Open University of Nigeria.*
[2]*Department of Computer Science, Michael Okpara University of Agriculture, Umudike, Nigeria.*
[3*]*Department of Sociology, Faculty of Social Sciences, Ambrose Alli University, Ekpoma, Nigeria.*

*chrismobibekwe@gmail.com

Received: 18 July 2025; Revised: 20 August 2025; Accepted: 05 September 2025; Published: 16 September 2025

Abstract - There is an intense and increasing rate of attacks on the cyber network of organizations. This paper examines the effect of cyber security on the organization network of selected commercial banks in Nigeria. Three research questions that were raised in line with specific objectives guide this paper. The theoretical framework is the Technology-Organisation-Environment (TOE) theory. A descriptive survey design is adopted. The sample size is one hundred and ninety-two (192) IT employees of the selected banks. A multi-stage sampling technique was used to select respondents, and the instrument for data collection was a structured questionnaire. Data were analysed using frequency, percentage, Likert scale, and mean ratings. Findings reveal that to a very large extent, there were attacks on the cyber network of commercial banks in the study area. It also shows that the attacks are to a large extent helping to improve the digitalisation operation of the banks, the protection of customers' data and the awakening of the importance of synergy in the fight against cyber attacks. It further indicates, amongst others, that strategies in place for the security of the network of commercial banks range from intensification of collaboration/synergy in information sharing, regular upgrading of cyber technological infrastructures, to customer sensitization on basic cyber attacks preventive measures. It concludes that until adequate safety measures are put in place, clients' monetary and other vital resources can be safeguarded. It, however, made vital recommendations for policy direction and implementation.

Keywords - Commercial banks, Cyber security, Network, Organization, Threat.

1. Introduction

The adoption and consistent use of the internet have become an integral part of human and organizational needs for not just communication, but for the facilitation of business activities. Digitization is helping organizations to sustain a wide range of activities, such as quick response, customer service and continuous business engagements (Federico, 2022). However, one threatening challenge to these lofty programmes is insecurity occasioned by attacks on cyberspaces. Cyber attackers are looking for avenues to exploit security lapses in organizational networks. Risks associated with the increasing reliance on digital platforms for transactions in contemporary times have heightened the importance of cyber security. In essence, the advancement in online technological transactions has brought about changes in business operations and at the same time, making

organizations more vulnerable to cyber attacks. When business organizations lose focus on the need to beef up cyber security programmes or fail to initiate continuous surveillance on their network system, cyber attacks become imminent (Aladenusi, 2021). Similarly, when there are bad elements in an organization, vital or sensitive information is likely to get into the hands of criminal syndicates.

Security is important for organizational success. It enhances the safety of data, information and protection of network systems from unauthorized access, usage, disclosure, disruption, modification and destruction (Okereafor, 2018). The author emphasized that the protection and safety of the organizational network is a vital business requirement. When the safety of data or information in an organizational database is guaranteed, it builds a positive image and confidence in customers. There would be less or no doubt in trusting such organization with sensitive information about oneself and resources. Cyberspace is a global network; hence, organizations undergoing digital transformation and lack sufficient capacity to safeguard the space continue to risk threats and attacks on their assets. The United States Federal Bureau of Investigation (FBI) reports that over 330,000 malware are created daily, with about 4,000 ransomware attacks launching on organizations (Hasan, Ali, Kurnia & Thurasamy, 2021). The most vulnerable of these organizations is the financial institution. This is not unconnected to the fact that they deal with money, which is the major attraction of cyber criminals.

The Boston Consulting Group reports that financial institutions are 300 times likely to experience cyber attacks than other organizations (Zakrzewski, Tang, Appell, Hardie, Hildebrandt, Kahlich, Mende, Muxí & Xavier, 2019). The porosity of the network and the lack of sufficient security measures in the space makes many banks prone to attacks, especially in developing nations. Kilani (2020) is of the view that digitalized organizational operations come with concern for protection and extra attention to technological infrastructures. Kilani argues that organizations in Jordan ranked high in data growth in cyberspace, while at the same time showing low commitment to technical control. This suggests that the organizations gave little to less attention to the security of data in their networks. This is disastrous given that a click by hackers can wipe away important organizational data and set a pace for regrettable reversal. This explains why Hasan et al (2021) submit that many business organizations in Bahrain lack cyber security readiness, hence, they perform poorly when compared with their counterparts in developed societies.

Nigeria has been experiencing a sharp rise in cyber security incidents. The fact that more businesses are moving online and storing sensitive data electronically without adequate measures for security calls for concern. In Nigeria, cyber criminality is in different categories and poses a serious threat to not just internet users, but also organizational data base. Ajibike (2019) argues that cyber attacks in the country range from hacking, software piracy, virus dissemination, phishing, cyber stalking, cyber defamation, and cyber plagiarism. Either they are trying to manipulate and defraud unsuspecting individuals, or they are targeting sensitive information of organizations to gain control. It is not just a security inadequacy but a breach of customers' trust for unauthorized persons to be in control of organizational network.

Statistics have shown that 71% of Nigerian organizations suffered cyber-attacks in 2021, while 44% spent an average $3.43 million as ransom to protect their businesses and secure sensitive data (Ikusika, 2022). Similarly, Kilani (2020) posits that many organizations are losing sensitive data to hackers, leading to huge cyber maintenance costs, which ordinarily would have been channelled to other projects. This suggests that cyber insecurity can pressure organizations to pay extra attention to their technological infrastructures, which is cost-effective. Makeri (2017) reports that the threat associated with cyber networks in Nigeria has become a national concern. Corroborating this view, Hasan et al (2021) submit that there is a rising spate of cyber attacks in recent times, which have negatively impacted the overall performance of many organizations. This suggests that cyber criminals are on the prowl, and the performance of an organization can be affected when such threats are not taken seriously.

Many organizations around the world, especially in Nigeria, are faced with the challenge of enhancing their cyber security to prevent or combat cyber network attacks. It is unnecessary to assume that merely uploading data on the web or storing it in smart devices guarantees safety. Criminal elements are taking advantage of the anonymity and privacy provided by the internet to unleash attacks on unguarded organizational cyber networks. Okereafor (2018) argues that the internet's nature and original design plan, which allows the freest possible exchange of information, data, and files, makes it vulnerable to attack. Consequently, organizations in Nigeria have recorded a series of cyber attacks and significant losses due to a lack of adequate security measures.

The persistence of the problem has led to loss of data, money in ransom and servicing costs of cyber networks, as well as a threat to the peace of customers. Aladenusi (2021) and Ikusika (2022) reports that the year 2020 and beyond witnessed a significant increase in cyber attacks and data breaches on SMEs, health institutions, and financial and non-financial institutions in Nigeria. The major targets of the attacks were individual devices, cloud tools and remote network infrastructures. The prevalence of attacks has resulted in a loss of confidence in e-commerce and cyberspace. As a result, many Nigerians are still unbanked and very comfortable keeping their money at home.

According to Ikusika (2022), cyber attacks on the network of notable Nigerian banks result in loss of over sixteen million naira and sensitive customers' data, such as Biometric Verification Numbers (BVN), and account information. Corroborating the report, Eyitayo (2022) cited the Nigerian Police Special Fraud Unit press release, which attributed the attacks to cyber loopholes in the network. Hasan et al (2021) were of the opinion that such attacks reveal the unpreparedness and incapacitation of most organizations in response to the threat. The obvious security lapses suggest why the hackers alleged that if they had wanted, they would have wiped out all the money in the accounts (Hasan et al, 2021).

The menace of cyber threats on organizational networks thrives where there are no responsive laws and effective counter-strategies. Various intervention approaches employed by both government agencies and financial institutions in Nigeria have not yielded the much expected cyberspace security. However, while Fatoki (2023) made effort to examine the influence of cyber security on financial fraud in the Nigerian banking industry, the study collected data from employees rather than IT experts and the study did not investigate the strategies employed in the banks in tackling security breaches; Ibikunle and Eweniyi (2013) in their study focused on organizations in Nigeria, relegated the banking sector. This suggests that much has not been done empirically in the country to ascertain the effect of cyber security on the commercial banks' network. To fill this apparent gap in knowledge, this paper examines the effect of cyber security on the organization network of selected commercial banks in Nigeria. Specifically, it seeks to;

- Determine the extent of attacks on the cyber network of commercial banks in Nigeria.
- Examine the extent to which attacks on the network of commercial banks have helped in strengthening cyber security in Nigeria.
- To determine the strategies or measures put in place by commercial banks in Nigeria for the security of their network.

2. Conceptual Review

Relevant key concepts guiding this paper are reviewed accordingly. The essence is to give a detailed explanation and a conceptualized meaning. The review is carried out under the following subheadings;

2.1. Concept of Cyber Security

Concerted efforts have been made by scholars to provide a concise definition of what cyber security entails. As there appears to be no universally accepted definition for the concept, there are some similar terminologies

that connotate what cyber security is. Ibikunle and Eweniyi (2013) conceived cybersecurity as the body of rules and regulations put in place for the guide, safety or protection of cyberspace. This definition recognizes the fact that a cyber network is a boundless space that, when left unmanned, can be tampered with and even cause colossal damage. Another view considered cyber security as every activity geared toward making cyberspace of organizations free from unauthorized interference or usage and enhancing the rightful persons' accessibility of needed information as when due (Okereafor, 2018). This view suggests that there is cyber insecurity when hackers and cyber criminals easily break into the cyber network of organizations, but it does not actually spell out measures that can be applied to repel such unauthorized access.

Cyber security is therefore conceptualized as the protection of digitalized systems and electronic information from attack (Ikusika, 2022). This definition made it clear that something vital or sensitive must be guarded jealously, especially from hackers and even unauthorized members of the organizational staff. This is because an unauthorized person can be a criminal syndicate that could leak or avail cyber criminals the information they need to rip the organisation's sensitive data. Pfleeger, Sasse and Furnham (2014) align with this view in their submission that IT employees within an organization are among the factors deeply influencing cyber insecurity. They maintained that many organizations take the training and retraining of their IT personnel for granted, thereby leading to insufficient awareness regarding the importance of cyber security.

Furthermore, cyber security is perceived as the rules and regulations put in place for the protection of the space of enterprising organizations (Hasan, Ali, Kurnia & Thurasamy, 2021). This view suggests that there have to be guidelines on organizational operations, including who accesses the sensitive digital database. This is giving that without well-spelt-out rules, there may easily be unauthorized interferences or usage, especially when there is no sanction. Therefore, for the proper safeguard of the organizational network, there must be guiding principles and sanctions for defaulters. This will not only ensure conformity but also bring about proper monitoring and guidance.

According to Ikusika (2022), security is a basic safety need of online and internet-connected business operations. Therefore, it is unsafe and unethical for a digitalized business venture to operate without adequate measures for a safer cyberspace. This is because virtually all business ventures are now either digitalized or in the process, or even basically have one thing or the other to do with the internet. Makeri (2017) argues that whether in government, industry (banking), or non-profit organizations, the internet has simplified business processes that even sorting, coding, editing, and customized and generic report generation have become the trend in real-time transactions. The increasing demand for internet connectivity and transactions brings the need for the safety of the space.

Based on the foregoing, cyber security can be defined as a body of guiding regulations that may be in the form of software and even legislation put in place to safeguard cyberspace. The essence is to prevent unauthorized access or to detect and repel external bodies that try to attack or infiltrate organizational network. An online database is the store and power house of many digitalized organizations, especially financial institutions; hence, the importance of safety in the space cannot be overemphasized.

2.2. Concept of Organization Network

Organization network can be described as a firm's internet connectivity or cyber network source. Hasan et al (2021) conceived organization network as the cyber connectivity that enhances the internet operations of organizations. According to them, the strength or safety of an organizations network may not only bring about competence and superior organizational performance, but also enhance its reputation.

Experts are of the view that poor network issues or design could bring about vulnerabilities in the control system. Afzal (2015) and Permann and Rohde (2013) posit that vulnerabilities in corporate networks are rapidly

increasing due to installation mistakes and issues in operation, configuration, testing, maintenance, and management. As a result, cyber attackers are infiltrating and breaching organizational network systems (Stouffer, Falco & Scarfone, 2010). Virtually every transaction today involves finance. Hence, a financial institution is one organization that cyber criminals target on a daily basis. To this effect, the need for adequate cyber security cannot be overemphasized. Technological applications that are geared toward securing an organizational network or database are essential for smooth operation.

2.3. Review of Empirical Studies

There have been research efforts toward cyber attacks and cyber security in various organizations. The majority of the studies were conducted outside of Nigeria, implying that there is a paucity of literature on the effect of cyber security on organization networks. In this digitization era, cyber security is critical to organizational performance, relevance and sustainability. A business organization can easily be edged out by competitors through obvious security lapses. This is because customers would always want a place where the protection of their resources is guaranteed. A study conducted by Gulyás and Kiss (2023), which examined the impact of cyber-attacks on financial institutions in Hungary, revealed that financial institutions suffered serious attacks from cyber criminals between 2020 and 2021. The attacks were largely attributed to the impact of the COVID-19 pandemic, which necessitated sole reliance on technological transactions. It further indicated that through remote access, Sberbank was attacked multiple times during the period using Trojan viruses. This suggests the severity of cyber attacks and the unpreparedness of the organization to tackle security threats. The implication is that investors who lost their hard-earned resources would be less likely to bank with the institution going forward.

Similarly, Fatoki (2023) assessed the influence of cyber security on financial fraud in the Nigerian banking industry. The results showed that financial institutions in the country experienced losses, decreased productivity, and vulnerability of ICT systems from time to time. It attributed the attacks to a lack of line manager and senior manager oversight, deviations from existing electronic processes and collusion between employees and outside parties, such as third-party services. This informs of the disturbing extent to which cyber attacks have permeated the Nigerian banking sector and the effect of unserious dispositions to the attacks.

In the United Arab Emirates (UAE), Solfa (2022) assessed the impact of cyber security and supply chain risk on digital operations in the pharmaceutical industry. Findings of the study showed that there was a significant positive association between cyber security and supply chain risk in digital operations. The study suggests that the issue of cyber attacks and the need for cyber security is not exclusively affecting the financial institution, but involves other business organizations. This suggests that cyber attacks are a phenomenon that cuts across digital sectors, especially where money and other sensitive data are involved. Similarly, research conducted by Hasan et al (2021) in Bahrain, on the factors influencing cyber security readiness of organizations and the effects on financial and non-financial performances revealed that cyber attacks have instilled cyber security readiness among organizational owners for improved performance. This implies that a cyber attack serves as a wake-up call to serious and committed organizations. In other words, it helps an organization to be up and doing, especially in trying to improve security measures.

Kilani (2020) examined the influence of cyber-security forces on internal organizational operations in Jordan. The results showed that cyber-security motivators (data growth, technology expansion, access to required resources, operational control, and technical control) indirectly affect solid internal processes. This was attributed to the consistency of technological infrastructure in an organization. It submits that effective security of organizational networks is lacking and therefore calls for sophisticated IT infrastructures as the main instruments of risk management. However, Okereafor (2018) analysed the patterns and severities of cyber attacks on routine organizational computer-based operations in Nigeria. Findings of the study revealed that the severity of cyber

attacks is much higher in the country and could be greater in the near future. This suggests there is a prevalence of cyber attacks and that organizational networks in Nigeria need to step up efforts to stem the tide. Furthermore, Ibikunle and Eweniyi (2013) conducted a study that provided an overview of cybercrime, cyber-security and their effects on cyber criminality in Nigerian organizations. The result showed that cybercrime has caused financial losses, loss of reputation, reduced productivity and vulnerability of Information and Communication Technology (ICT) systems in the country's digital organizations. It also indicated that the anonymity and speed of cyber technology complicate detection and investigation, thereby making it easier for cyber criminals to go uncovered for years. However, with the right technological measures and expertise, the activities of cyber criminals would not just be repelled but can be tracked down for prosecution.

2.4. Theoretical Review

This paper adopts the Technology-Organization-Environment (TOE) theory. The theory has been widely used in research to explain the interplay between technological usage and organizational environment. It equally helps to understand breaches or challenges often associated with the adoption of new technology. The TOE framework was developed in the field of information systems to explain how the adoption and use of new technologies are influenced by various factors, including the technological characteristics, organizational context in which it is used and the external environment in which the organization operates (Theory Hub, 2023). The relevance of the theory is in its ability to recognize both internal and external forces that jointly influence technological consideration, adoption and usage. In essence, it disconnected from sole attention to the possible usefulness of a technology or organizational services that its adoption may boast, but goes further to consider other forces. Hasan et al (2021) utilized this theory to evaluate the cyber security readiness of organizations and its influence on performance in Bahrain. He posits that cyber security readiness is an outcome of having the right personnel with the right skills and enabling the work environment to actualise core mandates.

While there seems to be a lack of committed readiness to combat cyber threats in many Nigerian organizations, especially the financial sector, there is also a need for strong legislation and institutions to help in the war against cyber attacks. Banks may not do much if cyberspace is left for them alone to secure. It may seem like a drop of water in an ocean, whose impact may not be felt. Therefore, it requires strong synergy because cyberspace is a vast and limitless world. However, the onus is on the organizations as well to hire experts with the requisite skills to man the space and not what inexperienced or unqualified persons should do. The theory also suggests that organizations are not supposed to be a hiding place for people of questionable character, given that the network space requires integrity to be able to safeguard, without which there is bound to be a compromise of customers' sensitive data.

3. Materials and Methods

A descriptive survey research design was adopted. The population of the study is three hundred and sixty-eight (368), and the sample size is one hundred and ninety-two (192) IT employees of commercial banks in South-East, Nigeria. This figure was statistically generated using Taro Yamane's (1967) formula. Through the use of multi-stage sampling techniques, respondents and banks were selected. First, South-East was stratified into its five States (Abia, Anambra, Ebonyi, Enugu and Imo) and their Capitals (Umuahia, Awka, Abakiliki, Enugu and Owerri), respectively. Through the use of paper balloting, Access, First Bank, and Keystone were selected from Umuahia, Abia State. Similarly, Ecobank, Fidelity and United Bank for Africa (UBA) were drawn from Awka, Anambra State, while Polaris, Union and Zenith banks were randomly selected in Abakiliki, Ebonyi State. The availability method was used to select the respondents. The instrument for data collection was a structured questionnaire, and content validation was carried out on the instrument by two research experts. Again, the Cronbach Alpha method was used to ascertain the instrument's reliability, and the index score obtained is 0.61, which is above the 0.50 acceptance benchmark. Data were analysed using frequency, percentage, Likert scale, and

mean ratings. The data analysis was processed with the aid of SPSS version 22. Out of the one hundred and ninety-two (192) copies of the questionnaire administered, one hundred and sixty-six (166) copies that were properly filled (representing an 86% response rate) were retrieved and used for analysis.

4. Results and Discussion

Data are presented, analysed and interpreted under the following tables. However, a detailed discussion of findings is presented in the last subheading of this section.

4.1. Socio-Demographic Data of the Respondents

The socio-demographic characteristics of the respondents, such as gender, age, educational attainment, years of banking experience, marital status and staff position were presented and analysed. The analysis is presented in Table 1.

Table 1. Distribution of respondents by Socio-Demographic characteristics

Demographics	Response (s)	Frequency (166)	Percentage (100%)	Mean (x)
Gender	Male	154	92.8	
	Female	12	7.2	
Age	Below 25	49	29.5	
	26-36	85	51.2	31
	37-47	23	13.9	
	48 & above	9	5.4	
Educational Attainment	FSLC	-	-	
	SSCE/WAEC	-	-	
	OND/NCE	94	56.6	
	HND/B.Sc/B.A	67	40.4	
	M.Sc/PhD	5	3.0	
Experience (Yrs.)	Below 5years	34	20.4	
	6-10	21	12.7	
	11-15	83	50.0	12
	16-20	18	10.8	
	25 & above	10	6.0	
Marital Status	Single	99	59.6	
	Married	64	38.6	
	Widowed	3	1.8	
	Separated/Divorced	-	-	
Staff Position	Senior Staff	35	21.1	
	Junior Staff	60	36.1	
	Contract Staff	71	42.8	

Source: *Field Survey, 2024*

Table 1 reveals that the majority of the respondents, 154 (92.8%), were males, while 12 (7.2%) were females. The majority of the respondents, 85 (51.2%), fell within the age bracket of 26 to 36, and the average age for the respondents was 31 years. At least 9 (5.4%) of the respondents were aged 48 years and above. Moreover, evidence shows that the majority of the respondents, 94 (56.6%), had OND/NCE, and this is followed by 67 (40.4%) who possessed HND/B.Sc/B.A. Those with postgraduate degrees were just 5 (3.0%), and none appear to have either FSLC or SSCE/WAEC as their highest educational attainment. The majority, 83 (50.0%), indicated having had between 11 and 15 15-years of working experience, with an average of 12 years in banking experience.

Furthermore, the table reveals that the majority of the respondents, 99 (59.6%), were single and 64 (38.6%) were married, while a small fraction, 3 (1.8%), were widowed. Above all, data revealed that the bulk of the respondents, 71 (42.8%), were contract staff, followed by 60 (36.1%) junior staff. The least of them, 35 (21.1%), were the senior staff.

4.2. Extent Cyber Network of Commercial Banks is Attacked

Table 2. Analysis of the extent to which the cyber network of banks is attacked

S/n	Statements	SA-5	A-4	UD-3	D-2	SD-1	N	X	Decision
i.	Cyber criminals' accessibility to sensitive data of customers to a very large extent	55	43	50	7	11	166	3.74	Accepted
ii.	Vulnerability of banks' IT facilities to a high extent	47	61	12	30	16	166	3.56	Accepted
iii.	It is to some extent heightening fears among financial institutions	49	57	26	20	14	166	3.64	Accepted
iv.	Leading to the theft of funds / information to a limited extent	68	18	19	21	40	166	3.31	Accepted
v.	To no extent discouraging customers from making transactions	39	17	13	25	72	166	2.34	Rejected
Grand Mean								**3.318**	

Source: *Field Survey, 2024*

Table 2 shows the extent to which the cyber network of commercial banks is attacked. A cursory look at the mean score of 3.74 suggests that, to a very large extent, cyber criminals access customers' sensitive data in the banks. It can again be observed that cyber attacks are to some extent heightening fears among financial institutions (x=3.64). Moreover, by a mean rating of 3.56, the respondents believe that to a high extent, banks' IT facilities are vulnerable to cyber attacks. Similarly, cyber attacks were to a limited extent observed through the mean score (x=3.31), leading to theft of funds/information in the banks. To see how customers' transactions were affected by these, a question was posed about whether it discourages customers' transactions, and the response shows that it does. The negative mean score of 2.34 suggests rejection of the statement and, by implication, implies that customers' transactions are to a significant extent affected by the attacks.

4.3. Extent Attacks on the Network of Commercial Banks in Nigeria have Helped to Strengthen Cyber Security

Table 3. Analysis of the extent to which attacks on the network of banks helped in strengthening their cyber security

S/n	Statements	SA-5	A- 4	UD-3	D-2	SD-1	N	x	Decision
i.	To a large extent, it is helping to improve the digitalization of operations	63	58	8	10	27	166	3.72	Accepted
ii.	Helps to a very high extent in helping banks to develop software that can repel malicious attacks	15	23	31	44	53	166	2.41	Rejected
iii.	To some extent, it helps to improve the protection of the personal data of customers	37	22	45	29	33	166	3.00	Accepted
iv.	Awakening of banks to the importance of synergy among them	48	60	51	6	1	166	3.89	Accepted
v.	Continuous effort in strengthening cyber loopholes in the networks	76	9	38	24	19	166	3.59	Accepted
Grand Mean								**3.322**	

Source: *Field Survey, 2024*

Table 3 presents an analysis of how attacks on the network of commercial banks have helped strengthen their cybersecurity. Based on the data in the table, the mean score of 3.89 suggests that commercial banks are awakening to synergize among them. It can again be deduced from the table that the mean score of 3.72 implies that, to a large extent, attacks on cyber networks are helping keep the banks on their toes, as there is constant improvement in the digitalization of their operations. This is affirmed by the positive mean (x=3.59), which indicates that there is continuous effort in strengthening cyber loopholes in the banks' network. This is validated by the mean output 3.00, which suggests that, to some extent, the attacks are helping the banks to improve the protection of customers' data with them. However, the effort to know if the challenge motivates the banks to develop software that can repel malicious attacks showed a negative mean response (x=2.41). This means that little to nothing is being done by the banks to develop locally made apps, different from what is bought from outside.

4.4. Strategies / Measures put in Place by Commercial Banks in Nigeria for the Security of Cyber Network

Table 4. Analysis of the strategies in place for the security of the cyber network of banks

S/n	Statements	SA-5	A-4	UD-3	D -2	SD-1	N	X	Decision
i.	Regular upgrading of sophisticated cyber technological infrastructures	52	34	2	32	46	166	3.08	Accepted
ii.	Floating of stringent legal rules to prevent cyber compromise among employees	73	41	28	14	10	166	3.92	Accepted
iii.	Intensification of collaboration/synergy in information sharing	81	62	1	22	-	166	4.21	Accepted
iv.	Capacity building of staff in cyber awareness and detection of attacks	42	54	18	40	48	166	3.66	Accepted
v.	Customer sensitization on basic cyber attacks and preventive measures	66	46	21	8	25	166	3.72	Accepted
Grand Mean								3.718	

Source: *Field Survey, 2024*

Table 4 analyses the strategies in place for the security of the cyber network of commercial banks in the study area. A cursory look at the table suggests that all the variables are accepted. This begins with the intensification of collaboration/synergy in information sharing among the banks, which bore a positive mean score of 4.21. This aligns with floating stringent legal rules to prevent cyber compromising among employees, with a mean rating of 3.92. There is also customer sensitization on basic cyber attacks preventive measures, with a mean of 3.72. It may be argued that this is necessary and a strategy of getting customers involved in issues pertaining to them. Similarly, a mean score of 3.66 suggests that the banks adopt capacity building of staff in cyber awareness and detection of attacks, and this may explain why there is regular upgrading of sophisticated cyber technological infrastructures among the banks (x=3.08).

4.5. Discussion

Having examined the effect of cybersecurity on the organizational network of selected commercial banks in Nigeria, findings revealed that to a very large extent, cyber criminals attack the network for sensitive data of customers in the banks. This aligns with findings of Boston Consulting Group in Zakrzewski et al (2019) that financial institutions are prone to cyber attacks than other organizations. This is understandable, given that they deal with money, which is the primary attraction of criminals. It explains why there have been losses of customers' sensitive information and even theft of funds. This is in agreement with Ikusika (2022), who reported that Access Bank and First Bank Nigeria lost over sixteen million naira (N16,000,000) to hackers. It further explains why it was observed that this menace heightens fears among the operators of financial institutions. This is understandable, given that an attack on customers is an attack on the existence of the banks. When customers

are discouraged or uncertain of the safety of their investments, they could easily opt for elsewhere or other primitive ways of saving.

Results of the study further showed that commercial banks are beginning to wake up to tackle the monster of cyber attacks on their network. This explains why there is rising synergy among them, and this suggests that no one organization can win the battle alone. It is something that requires cooperation and sharing of information, especially on the modus operandi and trend. The attacks are believed to be helping to a large extent in keeping the banks on their toes, as there is constant improvement in the digitalization of their operations. This explains why there is a constant effort to strengthen cyber loopholes in the banks' network. This corroborates Eyitayo (2022), who reports that hackers leverage cyber loopholes in the network of banks, especially when it is left insecure. Although there is no clear evidence that the banks are developing indigenous software that could help repel the attacks, it is heartwarming to note that they are making frantic efforts to strengthen the protection of customers' data.

Furthermore, findings suggest that in a bid to ensure the safety of the cyber network, commercial banks are now intensifying collaboration/synergy in information sharing. This is a commendable step in the right direction, emphasising the earlier submission that no one can win the war against cyber attacks alone. It therefore becomes imperative to synergize and network with others to be one step ahead of hackers. This is in tandem with the view of Gulyás and Kiss (2023) that canvassed for intensifying stronger international collaboration in information sharing to clamp down on cybercriminals or hackers. The finding on stringent legal rules to prevent cyber compromising among employees is germane, as evidence has shown that insiders often leak certain sensitive information to criminal syndicates for pecuniary gains. It becomes necessary for employees to be put on check to ensure non-compromise and integrity. The importance of capacity building and regular upgrading of cyber infrastructures in realizing this cannot be overemphasized. This is because frustration could make any staff member compromise and settle for a mess rather than uprightness. The result is that the banks are equally adopting sensitization as a strategy for enlightening customers on basic cyber attacks, and informing customers of the importance of customers to organisations. As a task that requires collective effort, customers are not to be left out.

5. Conclusion

Cyber operations have come to stay, and it is a vital tool for the effective service of customers of many organizations. The increasing risk and impact of cyber attacks on commercial banks, especially in Nigeria, have become a concern for stakeholders and the government. Negligence of these threats could amount to the collapse of an entire system and equally harm many. Money is the bane of development and the smooth running of any society. If left under the control or access of criminal elements, it poses a danger. Curbing cyber security breaches could help to increase public confidence in the financial system. Therefore, the security of commercial banks has to be strengthened to enable them to operate in a safer and secure environment. Until adequate security measures are in place, clients' monetary and other vital resources can be safeguarded. Based on findings and conclusions, the following recommendations are made;

- Financial institutions should continue and never relent in improving their cyber security efforts. This is because cyber criminals also do not slack, but are always busy seeking ways of having easy access to the cyber domain of organizations.
- There should be strong synergy among banks in sponsoring the development of indigenous software, like antivirus and counter-malware, that will help resist unwarranted invasion. This would promote local content creation, guarantee safety, and help uncover ingenuity among indigent IT practitioners.
- Customers' confidence in the banking system should continuously be strengthened. This is because once doubt or fear prevails, the aftermath effect could be misinformation that would make others pull out their

resources, thereby collapsing a banking system.

- Integrity should be prioritized in hiring bank staff. This is to avoid the recruitment of people of questionable character who may come into the system to wreck it with their criminal syndicates.
- Laws against cyber attacks, especially on financial institutions, should be strengthened by various relevant government agencies. They should be made public knowledge, and any breach should receive prompt and severe prosecution to deter potential criminals.

Data Availability

The unavailability is in observance of ethical rules on the protection of respondents' sensitive personal and organizational confidential details. However, in the event of a need for replicability, the raw data can be made available on request.

Authors' Contributions

The lead (first) author carried out the field work and research writing, the second author did the proofreading and some corrections, while the third author assisted in the data analysis and publication corrections/correspondences.

Acknowledgments

We acknowledge the selected banks and the respondents whose opinions culminated in very useful data that gives direction to this study.

References

[1] Muhammad Afzal, "*Human and Organizational Aspects of Cyber Security from a System Suppliers Perspective*," Master Thesis, Department of Industrial Information and Control Systems, Royal Institute of Technology Stockholm, Sweden, 2010. [Google Scholar]

[2] Sesan, Youth and Cybercrime in Nigeria, Punch Newspapers, 2019. [Online] Available: https://punchng.com/youth-and-cybercrime-in-nigeria/

[3] Tope Aladenusi, A Fresh Perspective Nigeria Cyber Security Outlook 2021, Deloitte, pp. 1-14, 2020. [Online] Available: https://www.deloitte.com/ng/en/services/risk-advisory/perspectives/nigeria-cyber-security-outlook-2021.html

[4] Eyitayo Johnson, Police Arrest Nigerian Fraudster Who Stole N1.87Billion After Hacking Into Bank's Server, Sahara Reporters, 2021. [Online] Available: https://saharareporters.com/2021/08/13/police-arrest-nigerian-fraudster-who-stole-n187billion-after-hacking-bank%E2%80%99s-server

[5] Jacob Obafemi Fatoki, "The Influence of Cyber Security on Financial Fraud in the Nigerian Banking Industry," *International Journal of Science and Research Archive*, vol. 09, no. 02, pp. 503–515, 2023. [CrossRef] [Google Scholar] [Publisher link]

[6] Federico Del Giorgio Solfa, "Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry," *International Journal of Technology Innovation and Management (IJTIM)*, vol. 2, no. 2, pp. 18-32, 2022. [CrossRef] [Google Scholar] [Publisher link]

[7] Oliver Gulyas, and Gabor Kiss, "Impact of Cyber-Attacks on the Financial Institutions," *Procedia Computer Science*, vol. 219, pp. 84–90, 2023. [CrossRef] [Google Scholar] [Publisher link]

[8] Shaikha Hasan et al., "Evaluating the Cyber Security Readiness of Organizations and its Influence on Performance," *Journal of Information Security and Applications*, vol. 58, 2021. [CrossRef] [Google Scholar] [Publisher link]

[9] Ibikunle Frank, and Eweniyi Odunayo, "Approach to Cyber Security Issues in Nigeria: Challenges and Solution," *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE),* vol. 1, no. 1, 2013. [Google Scholar] [Publisher link]

[10] May Robin Permann, and Kenneth Rohde, "Cyber Assessment Methods for SCADA Security," *15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference*, 2005. [Google Scholar] [Publisher Link]

[11] Shari Lawrence Pfleeger, M. Angela Sasse, and Adrian Furnham, "From Weakest Link to Security Hero: Transforming Staff Security Behavior," *Journal of Homeland Security and Emergency Management*, vol. 11, no. 4, pp. 489-510, 2014. [CrossRef] [Google Scholar] [Publisher link]

[12] Bamidele Ikusika, "A Critical Analysis of Cyber Security in Nigeria and the Incidents of Cyber-Attacks on Businesses/Companies", *SSRN*, pp. 1-19, 2022. [Google Scholar] [Publisher link]

[13] Yanal Kilani, "Cyber-Security Effect on Organizational Internal Process: Mediating role of Technological Infrastructure," *Problems and Perspectives in Management*, vol. 18, no. 1, pp. 449-460, 2020. [CrossRef] [Google Scholar] [Publisher link]

[14] Yakubu Ajiji Makeri, "Cyber Security Issues in Nigeria and Challenges," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 4, pp. 315-321, 2017. [CrossRef] [Google Scholar]

[15] Kenneth U. Okereafor, "Impacts of Cyber Attacks on Corporate Business Continuity: Fostering Cyber Security Consciousness in the Citizenry", *The 1st National Conference on Cybercrime and Cyber Security, Nigeria*, 2008. [Google Scholar]

[16] Keith Stouffer et al., "Guide to Industrial Control Systems (ICS) Security ", NIST Special Publication, vol. 800, no. 82 Rev. 2, 2011. [CrossRef] [Google Scholar] [Publisher link]

[17] Anna Zakrzewski et al., Global Wealth 2019: Reigniting Radical Growth, Boston Consulting Group, 2019. [Online]. Available: https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth