*International Journal of Arts, Languages and Business Studies (IJALBS), Vol.9; February, 2023; pg. 25 - 35*

# CYBERSECURITY ISSUES AFFECTING ONLINE BANKING AND TRANSACTIONS IN NIGERIA

**AUSTIN-OLOWO, OLUBUKOLA ANIKE; IKPEFAN OCHEI AILEMEN; LUKMAN BUSARI ALFA**
**Department of Accounting, Finance and Taxation,**
**Caleb University, Lagos, Nigeria.**

## ABSTRACT
*Online banking and transactions have become the trend of the century. Most transactions and businesses are done through the means of internet and other electronic devices as a result of globalization. However, threats of this innovation in banking and businesses have eroded its benefits due to insecurity. This paper investigated numerous cyber security issues affecting both online banking and online transactions in Nigeria with the objective of building the resilience of the financial system to these systemic risks. The researcher adopted both primary and secondary data in order to explore the old and new trends in cyber security affecting online banking and online transactions. Findings from this research revealed that: hacking into customer's account, delay in transferring money from one bank to another among others, do affect online banking and transactions in Nigeria. It is concluded that adequate security is essential for the thrive of online banking and transactions across the globe, especially Nigeria to enhance the growth of the economy. This study therefore recommends increased cyber security capacity building and sensitization seminars, engaging system penetration testers and frequent infrastructure/system review and upgrade among others in order to bridge cyber security gaps.*

**Keywords***: Cyber security, Online banking, Online transaction, Cyber-attack, Financial inclusion.*

## INTRODUCTION
### Background to the study
The twenty-first century technological advancement has no doubt brought about phenomenal transformation to the financial system and the entire global economy. Online banking and transactions in Nigeria have evolved over time with the introduction of credit and debit systems by an American banker named Biggins John in 1946 with his invention of Charge-It card, the first ever credit card. However, the connectivity of the world through internet has made perpetration of crimes easier for criminals (Kolade, 2022). Online banking and online transactions which started in the early 1980s in New York have thereby become a click at a fingerprint as a result of digital innovations, thus enhancing financial inclusion of the hitherto unreached in the rural and less urban areas of the world.

Cyber-security concerns the safeguarding of both hardware and software of a computer or digital network systems from harm through attack called cyber-attack. (Ezeji, 2020). It also involves the techniques of data protection or information architecture of an organization. There are various categories of cyber-attack, namely; malware, phishing, spoofing, among others. Investigation revealed that Cyber security issues affecting online banking and transactions include, but not limited to hacking into customers' accounts through personal details, lack of strong regulatory framework, inadequate budget, lack of information among customers, unauthorized debits, dearth of cyber security experts, "man-in-the middle", lack of trust, fear of fraud, among others. (Ezeji, 2022). The global cybercrime damage costs are; $190.00 per second, $11.4 million per minute, $684.9 million per hour, $16.billion a day, 115.4 billion a week, $500 billion a month and 6 trillion a year. Further, the indirect losses accrued from cyber security issues include; monetary equivalent of the losses and opportunity cost imposed on society (Ezeji, 2022).

Prior literatures in the likes of Accenture (2020), reported that companies spend an additional $2.4 million on average due to malware attacks. Nigeria ranked 16th in FBI (Federal Bureau of Investigation)'s report on global crime victims. Other empirical literatures revealed that in Nigeria, the total amount involved decreased to N18.94 billion at end of December 2018, from N19.77 billion at end of June 2018. Similarly, actual losses declined to N2.21 billion in the period under review from N12.1 billion in the first half of 2018. The Automated Teller Machines (ATM) and mobile money channels recorded the highest incidences of fraud. Subsequently in order to tackle this trend, bank customers were continually sensitized on safe banking practices while banks were encouraged to implement strong authentication controls and carry out comprehensive infrastructure risk assessments. Prior literature, Kolade (2022) reported that, despite the increased effort of the Central Bank of Nigeria in enhancing cyber security for the nation's financial industry, increased awareness, capacity development, and collaboration are still necessary to ensure cyber security resilience of the financial sector.

According to McKinsey (2022), Nigeria is home to over 200 Fintech organizations, not counting fintech solutions provided by banks and mobile network operators. The rapid growth in financial technology therefore increased the vulnerability of Nigeria to systemic risks, thereby creating the need to adequately safeguard the cyber security system, especially in the sensitive and all essential financial sector. Again, new service providers such as mobile money operators, payment service providers, fintech firms, and other financial services providers evolved numerous important digital components, including mobile applications, digital tokens, unstructured supplementary service data, and digital ledgers, all of which involve potential vulnerabilities and the increasing need for consumer security and trust.
In connection thereto, the United States Federal Bureau of Investigation had issued a warning to banks on a new trend of fraud known as the ATM Fraud or ATM Cloned Card fraud, which involve hackers accessing bank systems or payment card processors and altering data to withdraw large sums of cash within a short period. (June 4 2022: Financial Times).

In response to this warning, CBN carried out vulnerability assessments on all banks and payment system providers and directed the remediation of identified vulnerabilities on all ATM servers. CBN, 2022). Further, in the evaluation of the relationship between e-banking and cybercrime in Nigeria, Samphina.com.ng (2021) opined that stringent security control is paramount to the optimization of e-banking in Nigeria. Similarly, in India, empirical studies revealed that there is a positive relationship between IT usage and cybercrime related to online banking and this is mostly common in India among the youths. Victoria and Harrison (2020) identified lack of advanced technologies to strengthen cyber security and unsatisfactory legislative compliance as some of the issues affecting the Nigerian online banking and online transactions.

**Statement of research problem**

The security of our online banking and related transactions is threatened by various issues evolving on a daily basis such that Nigeria's image is being dented (Ezeji, 2022). Regrettably, majority of banking populace are not aware of measures in place to tackle these cyber security issues in Nigeria. According to FBI (Federal Bureau of Investigation), Nigeria ranked 16th on its report on global crime victims (FBI. 2020). Also, the total number of reported fraud cases in OFIs (Other Financial Institutions) stood at 754 at end of December 2018, while the actual loss of N120.98 million was recorded during the same period. (FBI, 2020). However, despite various measures by the government and private firms, these issues have not been adequately addressed. Hence, the urgent need to address these cyber security issues through increased awareness so as to strengthen the resilience of the banking industry against these systemic risks.

**Objective of the study**

The general objective of this study is to examine the various cyber security issues affecting online banking and online transaction in Nigeria with the specific objectives as follows:

1. To identify the cyber-security issues affecting online banking and related transactions in Nigeria.
2. To investigate the various measures in place to tackle these cyber-security issues in Nigeria.

3. To determine the adequacy of these cyber-security measures on the online banking and related transactions in Nigeria.

**Research questions**

The study therefore sought to answer the following research questions:

1. What are the cyber security issues affecting online banking and online transactions in Nigeria?
2. What safety measures could address these cyber security issues in Nigeria?
3. To what extent do these measures address the cyber security issues in Nigeria?

**Research hypotheses**

This study shall consider the following hypotheses:

Ho1: There are no cyber security issues affecting online banking and related transactions in Nigeria.

Ho2: There are no measures to tackle the effects of these cyber security issues in the banking and related transactions in Nigeria.

Ho3: The existing cyber security measures do not significantly impact online banking and related transactions in Nigeria.

**Scope of the study**

This study covered cyber security issues affecting online banking and online transactions across the globe with specific focus on Nigeria. Measures to address the various cyber security issues, and the adequacy of these measures. Primary data were obtained from cyber security related departments in Caleb University, Eco bank Nigeria Plc., and Sterling Bank Plc. due to proximity and good relationship with the researcher and secondary data from the 2020 Statistical Bulletin of the Central Bank of Nigeria to ascertain the value of digital financial services on the economy. The study is divided into five: Introduction, review of related literature, the methodology of the study, discussion of the result and the last is conclusion and recommendations.

**Significance of the study**

Firstly, this study is significant in exposing the various cyber security issues affecting online banking and online transactions in Nigeria.

Secondly, it is useful for the government and other financial institutions in curbing the challenges posed by online banking and online transactions.

Thirdly, this study is significant to the educating numerous bank customers and various customers using online transactions locally and internationally.

Fourthly, it is significant to the future forward of cyber security across the globe.

Finally, the study is useful for research students and researchers generally for further studies.

**Literature Review**

**Concepts and Conceptual Literature Review**

**The Concept of Cyber Security**

The concept of Cyber security in this study is the safeguarding of digital banking services and online transactions from adversity and hazards, such as information disclosure, theft, or disruption of services it provides. According to Kaspersky, 2022, it describes the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. The concept of cyber security which began in the 1980s in New York describes the protection of computers, networks, and electronic gadgets and information from threats and attacks.

**Online Banking**

Online banking is the provision of banking products and services through the internet by the use of digital devices such as telephones and computers. (Kolade, (2022). It is also an electronic payment system which enables customers of a bank or other banks to perform financial transactions through the bank applications

(Apps). Global report revealed that nearly four billion US dollars were lost to breaches in data security by business in 2016 while an average of 24000 records per incident was exposed. It was also reported in UK that it costs thirty-four billion US dollars per year to repair the damage done by hackers who penetrated security systems.

**Online transactions**

Empirical report revealed that the mid-1990s saw the introduction of online payments. The Stanford Federal Credit Union is credited as the first organization to offer their clients an online payment system, having first done so in 1994. Legend has it that the first-ever online purchase was a pizza from Pizza Hut! The cashless policy began in Lagos from January 2012, while the policy took effect in Rivers, Anambra, Abia, Kano, Ogun and the Federal Capital on the 1st of July 2013. The policy was implemented nationwide in July 2014.Online transactions are trade activities through mobile phones, computer networks, credit cards or automatic teller machines. Similarly, online banking refers to banking transactions through the use of internet, banking applications and websites.

**Cyber Attack**

A cyber-attack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Hackers (cybercriminals) use malicious code and software to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cyber-crimes such as financial information, healthcare record, and identity theft or system infiltration. According to Morgan (2019), cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.

**Cyber security Issues in Online Banking and Online Transactions**

Investigation from financial and cyber security experts and revealed some of the cyber security issues affecting online banking and online transactions as being among others: Malware, Spoofing, Unencrypted data, compromised data and unsecured third party services leading to reputational risk, reduced financial inclusion, and productivity/ monetary issues. Also unauthorized debits by hacking into customers account through phones, delay in transferring money from one bank to another, Spam emails, Trojan, Denial-of-service (DoS), Scareware, Phishing, Fiscal Fraud, State Cyber-attacks, Carders, False positives, key-logging, among others. (interview, 2022).

**Theoretical Review**

This study was anchored on complexity theory and transaction cost theory to strengthen the resilience of the Nigerian banking industry and populace to the risks of online banking and the reduction of transaction costs through online because knowledge is paramount to eradicating this social menace in Nigeria

**i. Complexity Theory (CT)** - Complexity theory (CT) relates to the interaction of systems to form a Network of heterogeneous systems. It provides an understanding of how computer systems relates and works in an organization or economy. It encourages innovation and real-time responses to change by allowing business units to self-organize. CT also describes the relationship between members of these systems as they give rise to the collective behavior and sheds light on how a system interacts with its environment (2021).

ii. **Transaction Cost Theory**

According to Williamson (1979), is a theory that suggests the use of organization's resources efficiently by minimizing the cost of transaction or operations. This theory was first proposed in 1937 by Ronald Coarse to explain the existence of firms and the costs incurred in the process of carrying out transaction. These costs vary depending on the intermediaries. The cost of online banking and transactions has been reduced due to technological advancement.

**Empirical Literature Review**

Empirical studies by Ezeji (2022), reported that several cyber threats are affecting online banking transactions and that cyber criminals have caused serious damage to the global economy. Kolade (2022) reported in his article that, despite the increased effort of the Central Bank of Nigeria in enhancing cyber-security for the nation's financial industry, increased awareness, capacity development, and collaboration are still necessary to ensure cyber-security resilience of the financial sector. Using six countries; namely Uganda, Nigeria, South Africa, Zimbabwe, Cameroon, and Ghana. McKinsey, in Financial Times (2022) reported that Nigeria is home to over 200 Fintech organizations, not counting Fintech solutions provided by banks and mobile network operators. The rapid growth in financial technology therefore increased the vulnerability of Nigeria to the systemic risk, thereby creating the need of adequate safeguarding of the cyber-security system especially in the sensitive and all essential financial sector. New service providers range from mobile money operators and payment service providers to Fintech firms and other financial service providers, a trend that is increasing the need to ensure consumer security and trust (Ezeji, 2022), These services come with numerous important digital components, including mobile applications, digital tokens, Unstructured Supplementary Service Data, and digital ledgers, all of which involve potential vulnerabilities. According to FBI report on global crime victims report, Nigeria ranked 16$^{th}$ among the nations with high rate of cyber-crime. Other empirical records revealed that $7.13 billion was the value of the data backup and recovery market in 2017. It will grow by 10.2% to reach $11.59 billion in 2022. (Markets and Markets, 2017). Survey showed that 61% are concerned about ransom ware, another 61% are concerned about social engineering attacks, and 60% about crypto jacking. (Acronis, 2019). Further records showed that 97% of businesses back up their data at least once a year. Of these, 86% perform backups monthly, weekly, or daily. (Acronis, 2019). According to IT experts, the technologies that bring the most risk in terms of data loss are ransom ware (42%), mobility/BYOD (38%), and social media use (9%). (Storage Craft, 2020). In addition, 39% of small- and medium-sized businesses do not have contingency plans in response to cyber-attacks and data breaches. (Ponemon Institute, 2019). Facts also revealed that up to 93% of small businesses store their data or backups in the cloud. (Unit rends 2019). Samphina.com.ng in the evaluation of the relationship between e-banking and cybercrime in Nigeria opined that stringent security control is paramount to the optimization of e-banking in Nigeria.

Victoria and Harrison (2020) identified lack of advanced technologies to strengthen cyber security and unsatisfactory legislative compliance as some of the issues affecting the Nigerian online banking and online transactions.

**Gap in Literature**

Paul Jackson from Kroll highlighted the 10 gaps in cyber security that organization face, such as unpreparedness, unknown threats, infiltration of organization's network, lack of monitoring, openness to fraud, mobile/home/travel security, third party/vendor risks, incident handling, internet of things, people risk. Other researchers from science, finance, engineering, and information technology have also investigated cyber security issues affecting online banking and transactions in the past and present, but some of their findings keep getting out of date as experts expect a cyber-attack attempt every 11 seconds in 2021 and beyond, which is twice the rate back in 2019. (Cybercrime Magazine, 2019). This therefore necessitates the need to keep investigating new trends in cyber security affecting online banking and transactions. This study therefore fills the gap in literatures by identifying recent trends in cyber security issues using primary data of interviews and questionnaires.

*2.5 Stylized facts*

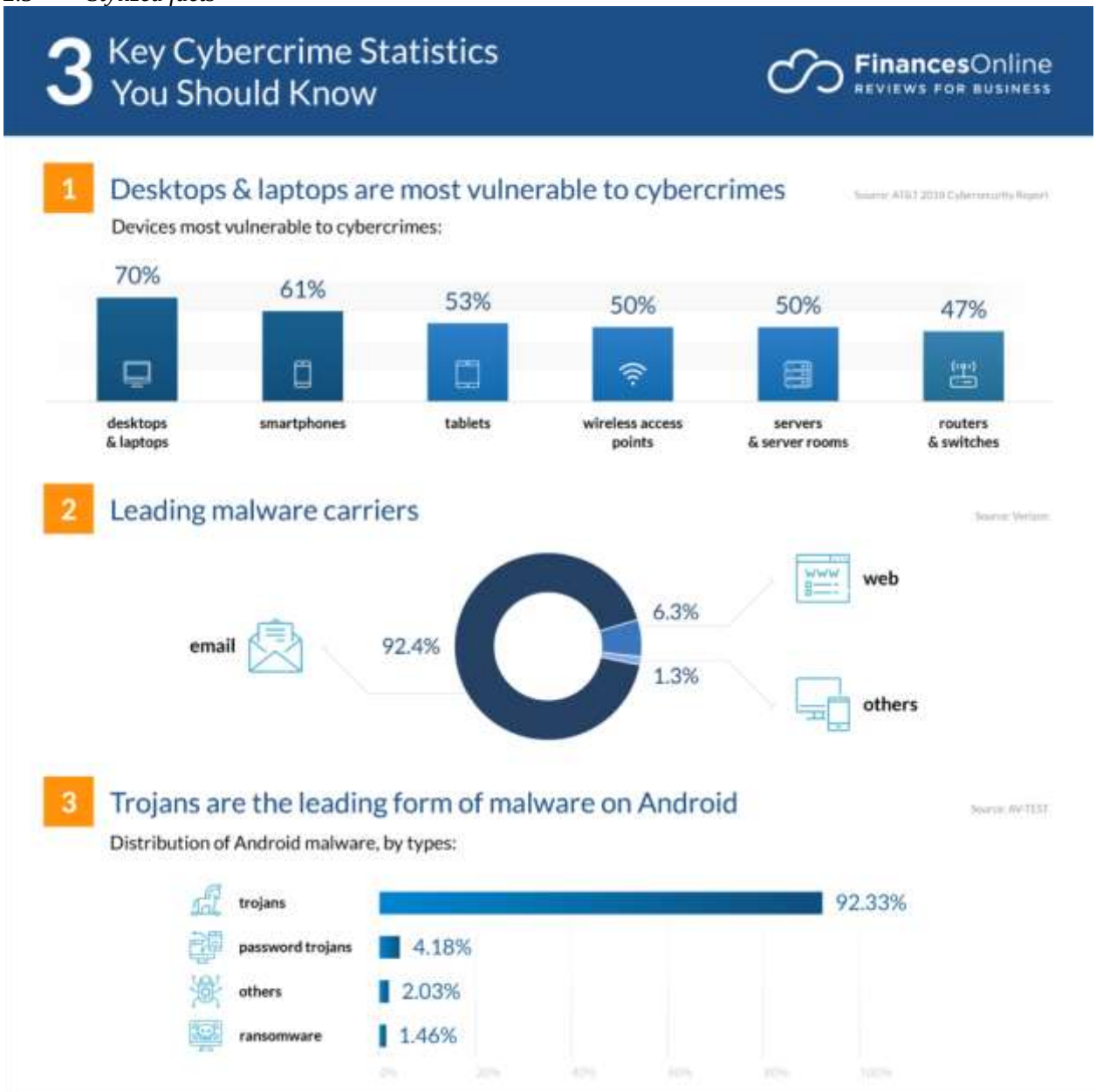
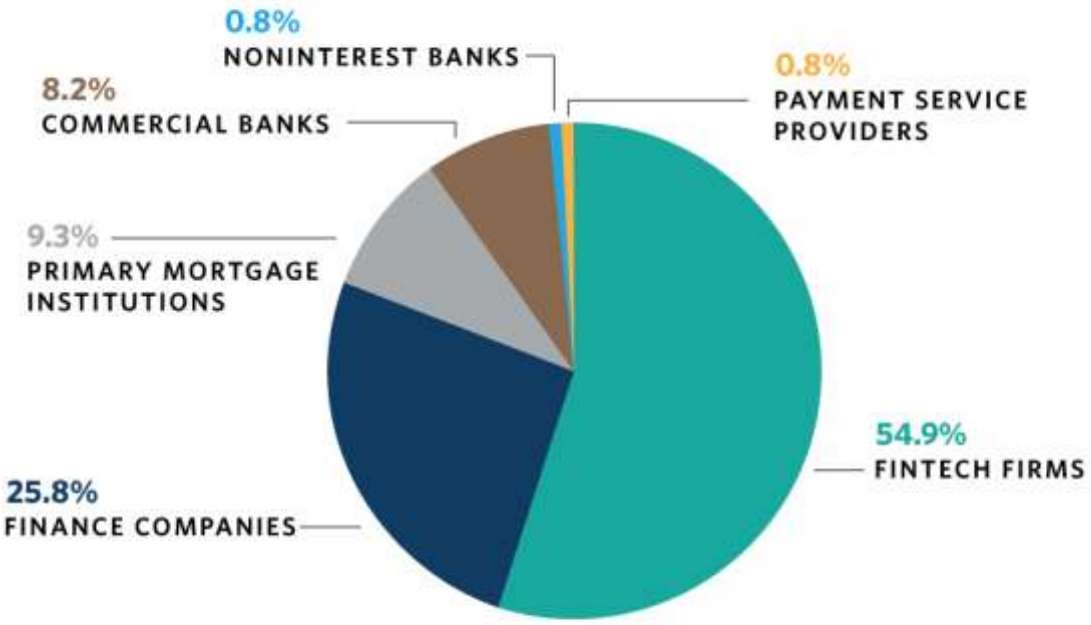


FIGURE 1
**An Overview of Nigeria's Financial Space**




SOURCE: Central Bank of Nigeria, "List of Deposit Money Banks as at September 30, 2021"; Kola-Oyeneyin, Kuyoro, and Olanrewaju, "Harnessing Nigeria's Fintech Potential"; Central Bank of Nigeria, "List of Financial Institutions – Micro-Finance Banks"; and Central Bank of Nigeria, "Financial Institutions."

NOTE: Due to rounding, the numbers may not add up to 100%.

**Future Forward in Cyber Security**

Companies will continue to face the threat of cybercrimes to their business and customers. Here are the current and future preparations

- From 2020 to 2025, spending on cyber security will exceed $1 trillion. (Cybercrime Magazine, 2019)
- The cyber-security market will grow by 12% to 15% growth through 2021. (Cybercrime Magazine, 2019)
- Microsoft is quietly becoming a cyber-security leader by acquiring Cyber X, a cyber-security solutions company, for a rough value of $165 million. (The Motley Fool, 2020)
- Experts expect a cyber-attack attempt every 11 seconds in 2021, which is twice the rate back in 2019. (Cybercrime Magazine, 2019)

**Methodology**

**Research Design**

The study adopted survey research design where representative percentage of the whole population is drawn. It is a systematic collection of data through the use of questionnaire, and the data generated is presented and analyzed in a way that describes the cyber security issues, preventive measures, and the degree of adequacy of these measures. This study employed both descriptive and inferential statistics in analyzing the data.

Descriptive statistics is an event or outcome of events that are described without drawing conclusion(s). It is primarily concerned with the collection, organization, summarizing, analysis and presentation of an array of qualitative and quantitative data (Morgan, 2019. The research design utilized for this study is descriptive in nature for analyzing data on cyber security issues affecting online banking and online transaction in Nigeria.

**Population of study**

The study population of over 300 employees consisting of financial experts, security experts from criminology department, cyber security experts from computer science department, information technology expert from Caleb University, Lagos for ease of access to information.

**Study Sample**

Random sampling of the population of study were carried out and to ensure speed and accuracy of response to the questionnaires, 5 respondents from each of these categories of relevant respondents that is, financial experts, security experts, cyber security experts, information technology experts from Caleb University were selected.

**Model Specification**

The model used in this study were econometric model expressed as: Y is a function of X
That is independent variable cyber security is a function of dependent variable online banking and online transactions. Y = fX
Mathematically,

i. OB&T = fCB

Hypothetically,

i. OB&T > CB (Null hypothesis i)
ii. OB&T > MCB (Null hypothesis ii)

Where
OB&T represent online banking and transactions
> represent greater than
CB represent cyber security issues
MCB represent measures of cybersecurity
Summarily:
Equation i above represents: Online banking and transaction is greater than cybersecurity issues, hence no effect of cyber security issues on online banking and transactions. While Equation ii represents online banking and transactions greater than cybersecurity measures, hence no adequate measures to tackle cybersecurity issues.

**Estimation Techniques**

Analysis of data were carried out using descriptive statistics in form of simple frequencies and percentages.

**Validity and Reliability of Research Instruments**

Research instruments were validated through content validity. Content validity assesses whether a test is representative of all aspects of the construct. The well-structured instrument drawn from the research questions were subjected to experts in the relevant field of study and the results compared with previous studies. The research was also tested by using t-test and re-test method for consistency.

**Data Presentation & Analysis**

Description of the variables
In this study, cyber security is the independent variable while online banking and online transactions are the independent variables. The effectiveness of online banking and online transactions is dependent on the

security of its cyber or network and information system. To answer the three major research questions in this study, the following data are hereby presented.

**Discussion of Findings**

From the administered questionnaires and based on the objectives of the study, the followings were found:

**Research Question 1: What are the cyber-security issues affecting online banking and transactions in Nigeria?**

100% of respondents according to Table 1 agreed that there are several cyber-security issues affecting online banking and transactions in Nigeria. Responses from financial experts revealed that these include unauthorized debits, lack of adequate budget for cyber-security by government, private firms, and individuals, malware, spoofing, unencrypted data, compromised data, unsecured third party services leading to reputational risk and reduced financial inclusion, reduced productivity and monetary losses. Other responses from banking industry also mentioned; ATM fraud, Phishing, hacking through social media as challenging cyber-security issues. Responses from security and criminology experts revealed: Hacking into customers account. delay in transferring money from one bank to another, fear of fraud due to the vulnerability of customers and organizations to the antics of criminal elements, cyber terrorism premeditated, politically motivated act against information, computer systems, computer programs, and data which results to violence against non-combatant targets, cyber warfare directed to cripple telecommunication, critical infrastructures and computer networks.

From the cyber security experts, it was revealed that phishing, impersonation of characters, codes, among others, are some of the cyber-security issues affecting online banking and transactions in Nigeria. These findings also align with the assertion of McKinsey in the Financial Times (2022) and could be tackled by the character-based ethical theory of Howard (2017).

Responses from the information and communication technology (ICT) experts showed that Denial of Service, Malware. Spam e-mails, among others, are some of the cyber-security issues. This supports complexity theory of inter-related systems in online banking and transactions.

**Research Question 2: What are the measures in place to address these cyber-security issues?**

Financial experts suggested cyber-security capacity building and sensitization seminars, user access enhancement, encryption and firewalls, regular vulnerability assessment, system penetration testers, frequent infrastructure/ system review and upgrade, Cooperation between bank operators and regulators, public awareness and other safety measures which support the conclusion of security and criminology experts opined non-disclosure of transactions to unauthorized persons, keeping cell phones safe, regular interface with banks, collaboration of banks and customers to keep information process alive, prompt reporting of infractions to the relevant stakeholders, building of trust, and consistent upgrade of systems to reflect the emerging realities, forensic investigation of cyber-crimes which requires the investigator to safe keep and identify physical evidence retrieved from computer and cyber system used in committing the crime as measures to address cyber-security issues in the Nigerian online banking and transactions.

**Research Question 3: To what extent do the measures in place address these cyber-security issues?**

The following findings are based on the above research questions by cyber-security experts (Table 3 in Appendix). In effect, the measures would be very adequate if regularly observed. The findings were supported by financial experts. However, Information Communication Technology (ICT) experts indicated rarely adequate due to non-observance of these measures.

**Summary of Findings**

This study on "Cyber-security issues affecting online banking and online transactions in Nigeria" revealed the followings:

That several cyber-security issues such as unauthorized debits, lack of trust, fear of fraud, use of malware to hack into customers account, identity theft, cyber-crime, cyber terrorism, inadequate budget for cyber-

security, lack of adequate cyber-security professionals affect online banking and related transactions in Nigeria. These findings support the works of Salami (2018), Kolade (2020), and Ezeji (2022). Again, phishing, scamming, man in the middle attacks, key-logging, hacking through social media. Delay in transferring money from one bank to another, ATM cloning, among others are some of the cyber-security issues affecting online banking and online transactions in Nigeria which could be eroded by ethical theories of consequential, virtue, and deontology by Howard (2017) and Cybercrime Magazine (2019).

That cyber-security measures like enactment and implementation of cyber-security laws, constant training of professionals, sensitization seminars, less exposure to social media, anti-malware software, back-up systems for retrieval, prompt reporting to appropriate authorities, prosecution of offenders, constant system and facilities upgrade, non-disclosure of details to unauthorized persons, financial literacy, community collaboration, and stakeholders co-operation among others are in place to build the resilience of the Nigerian financial system to this systemic risk as reported by Victoria and Harrison (2020).

That the above safety measures are very adequate, and have been working to some extent but not as effective as it should be due to lack of awareness and implementation as supported by Ezeji (2022) and Kolade (2020).

That digital financial services tools such as ATM, POS, WEBPAY, and MOBILE BANKING have significant positive impact on the gross domestic product of Nigeria as shown on payment system table of CBN's Statistical Bulletin (2021), hence the need to implement adequate cyber-security safety measures to build the Nigerian financial system's resilience to the associated risks of online banking and online transactions which supports transaction cost theory.

## Conclusion & Recommendations

### Conclusion

In conclusion, this study examined cyber-security issues affecting online banking and online transactions in Nigeria with specific objectives of highlighting some of the cyber-security issues, measures in place, and the adequacy of the measures to address these issues. The study utilized both primary and secondary data to source data for the research and findings revealed some of these issues, measures in place and the adequacy of the safety measure to address the issues if implemented.

### Recommendations

This study therefore recommends the followings:

Consistent monitoring of transactions from both the sender and the receiver.

i. Regular changing of PINs and PASSWORDS to secure online accounts.
ii. Employment and constant training of cyber-security experts or professionals.
iii. Building and implementing cyber-security framework that will reduce the vulnerability of stakeholders to online banking and online transactions.
iv. Less exposure of customers personal to social media such as displaying their emails, account details, and others.
v. More awareness and integration of information technology solutions for security.
vi. Adequate budget for cyber-security by the Government and private organizations.
vii. Cooperation between the bank operators and regulators on the emerging risk of cybercrimes in online transactions to enhance financial system stability.
viii. Increased sensitization programme for stakeholders among others, can safeguard some of these cyber security issues affecting online banking and online transactions in Nigeria.

## REFERENCES

Accenture Fiscal 2020 Annual Report.

Acronis True Image 2019 for PC: Delivering Easy, Efficient, Secure Cyber Security Protection. Total cyber protection. Acronis.com.

Central Bank of Nigeria (CBN)'s Statistical Bulletin 2021.

Cybercrime Magazine, 2019. Official Annual Cybercrime Report – A 2019 report from Cyber security Ventures.

Ezeji, 2020: Disruptive Technology: The Contestation between Criminal Justice and the Cybercriminals on the Cyberspace.

Howard, A.G., Soniya, S. Madasu H., Shantaram V. (2017). Mobile Nets: Efficient Convolutional Neural Networks for Mobile Vision Applications. https://arxiv.org/abs/1704.04861

John C, Biggins, 1946. An American Banker and Inventor of Charge-It Card.

Kolade, E. (2022). Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security. The CBN 's Cybersecurity Capacity Development, and Financial Inclusion project, acarnegieendowment.org May 13, 2022,

Kuyoro A.F. (2017). Measuring Financial Inclusion and the Fintech Revolution. World Bank Publication, 19 Apr 2018. books.google.com.ng

McKinsey J. (2022): "The Firm: The Story of McKinsey and its Secret Influence on American Business" (Simon & Schuster). https: wikic2com: McKinsey. The Financial Times.

Markets and Markets, 2017. Revenue Impact Model. 'What's Your Growth Innovation Index? Markets and makets.com.

Morgan, S, 2019. Editor-In-Chief Cybersecurity Ventures. 2019 Official Annual Cybercrime Report.

Ponemon Institute 2019. Exclusive Research Report – 2019 Global State of Cyber-security Innovation. https://www.cisco.com

Ronald G. Wayne, 1976. A retired American electronics industry businessman. A co-founder of Apple Computer Company.

Salami, 2018: A Review Paper on Cyber-Security – IJERT www.ijert.org/a_review.

Storage Craft, 2020. PC Magazine Editors' Choice award winning. StorageCraft@Shadow Protect. https://www.storagecraft.com

The Motley Fool, 2020. Motley Fool Stock Advisor.

Unit rends 2019. All-In-One Enterprise, Backup and Continuity Solutions. https://www.unitends.com.

Victoria S. Harrison (2020), Realigning Philosophy and Wisdom in the 21st Century. Algemeen Nederlands Tijdschrift voor, Wijsbegeerte 112 (3):325-340 (2020).

Williamson (1979) Transaction-Cost Economics: The Governance of Contractual Relations. Journal of Law and Economics, 22, 233-261. http://dx.doi.org/10.1086/466942