

Cyber Security Cost and Financial Performance of Deposit Money Banks in Nigeria.

Nnam, Hilary Ikechukwu, PhD.

*Department of Accounting,
Alex Ekwueme Federal University Ndufu-Alike, Ikwo, Ebonyi State*

Okoro, Chinonso Churchill, PhD.

*Department of Accounting,
Michael Okpara University of Agriculture Umudike*

Churchill-Okoro, Chinwendu Judith

*Department of Accounting,
Michael Okpara University of Agriculture Umudike*

Bamwa, Blessing, PhD.

*Department of Accounting,
Ignatius Ajuru University of Education, Rumuolumeni*

Date of Submission: 28-03-2026

Date of Acceptance: 08-04-2026

ABSTRACT

The study focused on cyber security cost and financial performance of deposit money banks in Nigeria. Cyber security cost was measured using e-technology/communication cost while financial performance was measured using return on asset, return on equity and earnings per share. Ex-post facto was adopted as the research design of the study. The data were collected through secondary source from annual report and account of the selected deposit money banks. The population of the study is made up of 14 listed deposit money banks while the sample size of 10 deposit money banks was derived using purposive sampling based on availability of data. The data collected were analyzed using ordinary least simple regression analysis. The result from the first hypothesis revealed that cyber security cost has no significant effect on return on asset of listed deposit money banks in Nigeria. The result from the second hypothesis revealed that cyber security cost has a significant effect on return on equity of listed deposit money banks in Nigeria. Finally, the result from the third hypothesis revealed that cyber security cost has a significant effect on earnings per share of listed deposit money banks in Nigeria. Based on the findings, the study concludes that cyber security cost has the tendency of influencing the financial performance of deposit money banks in Nigeria. Therefore, the study recommends that banks should take more cost-effective steps and

more reliable technologies that do not offer loopholes for illegal activities to take place. There should also be more investment in prevention and detection techniques, because banks invest significant sums in the production of these goods.

Keywords: Cyber security cost, information and communication technology, return on asset, return on equity, earnings per share.

I. INTRODUCTION

One important factor in improving banks' performance is electronic banking, or "e-banking" (Siddik, et al., 2016). The customer uses e-banking, a banking method, to execute transactions electronically via the Internet (Gupta, 2019). The increased financial outcomes of any e-bank determine its productivity (Jepchumba & Simiyu, 2019). According to Governance (2019), financial performance is a metric that quantifies a company's ability to use its resources efficiently and make money from its primary economic activity. Product innovation is measured by how well new products are developed and then introduced, either as improved versions of the prior product or service, or as whole new ones (Henri & Wouters, 2019). With the aid of e-banking services, customers may readily use such services as automated teller machines (ATMs), personal digital assistants (PDAs), e-wallets, e-kiosks, and so forth (Söylemez & Ahmed, 2019). Enhancing the market share and company

growth of the financial industry is the aim of electronic transaction services. The main issue affecting the financial growth of e-banking is cyber security or computer crime (Nazaritehrani & Mashali, 2020). Cybercrime is characterized as illegal action involving computers or the Internet (Yar & Steinmetz, 2019). Electronic crime can be variably referred to as computer crime, high-tech crime, digital crime, e-crime, and cybercrime (Usman, 2017).

According to Padmaavathy (2019), computers are utilized in cybercrimes as either a tool for committing crimes, a recording device, or as targets for crimes. Computers may either be used to store data or as a tool to aid commit crimes like intellectual property theft, which is against the law for owners to possess. According to Njoroge (2017), the costs associated with cyber security include: a) prevention and detection costs (firewalls, filters, antivirus), b) response costs (damage to reputation), c) indirect costs (loss of customers), and d) development costs (maintenance and quality). Research has indicated that the expense of cyber security has a significant impact on an organization's ability to innovate new products (Jepchumba & Simiyu, 2019). Research has furthermore demonstrated that the scant number of research carried out focused on the financial performance of electronic banking and the cost and expenditure of cyber security (Desta, 2018). Furthermore, Ahmed (2018) notes that there is no research in Nigeria that quantifies the correlation between the expense of cyber security and the financial success of online banks. The Forbes (2020) study projects that global investment on risk management and information security systems will reach \$131 billion in 2020. By 2022, that amount is expected to increase to \$174 billion, with endpoint security accounting for almost \$50 billion of that total. Cloud security platforms and apps are expected to dominate all information & security risk management systems categories and see a compound annual growth rate (CAGR) of 36.8%, with sales expected to increase from \$636 million in 2020 to \$1.63 billion in 2023. Application security is predicted to grow at a 9.7 percent compound annual growth rate (CAGR) from \$3.4 billion in 2020 to \$4.5 billion in 2023. Security services are predicted to generate \$66.9 billion in revenue this year, up from \$62 billion in 2019. The majority of the information security unit's cyber security analysts are now irritated with their work checking security records, stopping attempted violations, and looking into possible fraud instances (Columbus, 2020). In order to determine the percentage of artificial intelligence (AI)-based computer security businesses from different nations,

such as Austria, Germany, France, Italy, India, the Netherlands, Sweden, Spain, the United States, and the United Kingdom, Cap-Gemini performed a poll in 2019. Senior IT leaders in the field of cyber security provided the information. Sixty-nine percent of top executives worldwide think AI and machine learning are critical for responding to cyberattacks. All told, 79 percent of senior utility IT managers, 68 percent of retail managers, 64 percent of automotive managers, 61 percent of consumer goods managers, 75 percent of banking managers, 69 percent of all industries, and 80 percent of telecommunications managers believe that their company will not be able to respond to cyberattacks without artificial intelligence.

According to Njoroge (2017), the banking industry is devoting a substantial portion of its budget to cyber security in an effort to reduce or manage cybercrime. Cybersecurity is the process of preventing hostile assaults on computers, servers, networks, mobile devices, electronic systems, and data. It also involves securing a computer network against intruders, such as opportunistic malware or targeted attackers (Bada, Sasse & Nurse, 2019). The price that must be paid in order to purchase or acquire internet security in order to defend against cyberattacks is known as the cyber security cost (Njoroge, 2017). Cui, Wang, and Yue (2019) identified three categories of cyberattacks: a) rampping attacks, or rectangles; b) random attacks, or triangles; and c) scaling attacks, or circles. These categories include password attacks, sub-query language (SQL) injection, denial of service (DoS) attacks, spearphishing and phishing attacks, malware attacks, and so on.

The amount spent on IT security in 2019 reached a record \$124 billion globally, with a significant portion going toward information security products and services, particularly in the following areas: identity access management (\$9.8 billion), consumer security software (\$6.4 billion), data security (\$3.1 billion), application security (\$2.7 billion), other information security software (\$2.1 billion), security service (\$58.9 billion), infrastructure protection (\$24.1 billion), network security equipment (\$12.4 billion), and cloud security (\$0.3 billion).

According to the previously stated research, the cost of cyber security has a significant impact on an organization's performance (Jepchumba & Simiyu, 2019; Njoroge, 2017). Research has also shown that the small number of studies that have been done on the subject of cyber security expenditure and cost as well as the financial performance of electronic banking (Desta, 2018; Rathore, 2016; Fianyi, 2015). Furthermore, Ahmed

(2018) notes that there is no research in Nigeria that quantifies the correlation between the expense of cyber security and the financial success of e-banking. To the best of the author's knowledge, no study has yet taken into account the role that product innovation plays in mediating the link between cyber security costs and the financial success of online banks, specifically in Nigeria. Thus, the study calculates the correlation between the expense of cyber security and the profitability of Nigerian e-banking. Therefore, main objective of the study is to examine the effect of artificial intelligence on accounting profession. The specific objectives are:

- (i) To examine the effect of cyber security on return on asset of listed deposit money banks in Nigeria.
- (ii) To determine the effect of cyber security on return on equity of listed deposit money banks in Nigeria.
- (iii) To examine the effect of cyber security on earnings per share of listed deposit money banks in Nigeria.

II. REVIEW OF RELATED LITERATURE

2.1 Conceptual Framework

2.1.1 Cyber Security

Cyber security refers to a series of practices and activities fashioned out with a view to ensuring the protection of personal and organizational data, information and networks from all possible threats whether internally or externally induced (Beck, Chen, Lin, C. & Song, 2014). These threats could include unauthorized access and disclosures, misuse of data/information, network hacking and organized attacks in the form of the introduction of malware and similar extraneous viruses (Sheth, Bhosale S., Kurupkar, 2021). According to Li and Liu (2013), cyber security measures can be broadly categorized into five main types namely: measures focusing on application security, network security, operational security, cloud security, user training and information security. Further broken down, some of these measures include password and authentication protocols, firewalls and data encryption methodologies, malware scanners and the use of anti-virus software (Kashmari, Ahg, & Nayebayzdi, 2016). Cyber security is often used interchangeably with the term 'information security' because according to the International Telecommunications Union (Ojeka, & Egbide, 2017), the chief objectives of cyber security revolves around ensuring the confidentiality, integrity and availability of information in the right amount, place and to the right person. This CIA (Confidentiality, Integrity and Availability) triad is considered very germane

for the financial services sector into which deposit money banks belong because of the sensitivity of data and information in the hands of handlers as well as the far-reaching consequences that breaches in them hold for the industry and the economy at large. For example, according to the 2020 report of the electronic fraud tracker ('Nigerian Electronic Fraud Forum'), the total value of cyber induced electronic fraud was in excess of N6.1 billion as at 2019. This thus provides the basis for the renewed focus by deposit money banks to strengthen their cyber security architecture via the instrumentalities of a more robust risk management framework and consistent bank monitoring in line with regulatory requirements (CBN, 2017). Specifically, the guidelines provide inter alia that each deposit money bank must employ "a risk management system to reduce the incidence of significant adverse impact" as well as put in place metrics for effective monitoring.

2.1.2 Cyber Security Cost

Security is a journey, not a destination. The security of computer systems and networks from theft or harm to their devices, software or electronic records, as well as from the interruption or misdirection of the services they offer is computer security, cyber security or information technology security (Khari, Shrivastava, Gupta, & Gupta, 2017). Following are some cyber security cost

Prevention and Detection cost

In addition to security awareness training, this security feature, which focuses on keeping harmful malware out of the device, involves antivirus, firewall and email filtering solutions. Intrusion prevention mechanisms and network management resources are used in this security function, which focuses on becoming conscious of security issues as soon as possible (Njoroge, 2018).

Indirect cost/negative image cost/Negative brand image costs

Indirect losses are the monetary equivalent of the losses and opportunity costs levied by cybercrime on financial entities (Njoroge, 2018). Examples of indirect losses include: lack of interest in online banking, resulting in decreased electronic transaction fee income, and increased costs for branch workers maintenance and cheque clearing facilities.

Response cost

Direct losses to individuals and firms (including catastrophe recovery response expense and market survival) and indirect losses resulting from

diminished market utilization of innovation performance and investment expenses by weakened competition are taken in to consideration in the response strategies. Consequential costs are those that have specifically impacted the banking company (Njoroge, 2018).

Developmental and maintains cost

Quality and repair expense was included in the developmental expense (Njoroge, 2017). Quality and maintenance costs are both a subset of production costs and have a direct influence on e-banking 's product innovation and financial results (Njoroge, 2017).

2.1.3 Cybercrime

Cybercrime is rising dramatically in today's engineering environment (Malik & Choudhury, 2019). Hackers on the Internet take use of people's private information for their own gain (Nurse, 2018). They venture further into the dark web to buy and sell illegal products and services (President, 2019). According to Tsakalidis and Vergidis (2017), cybercrime is defined as a crime when a machine is the target or is employed as an offensive weapon. A cybercriminal can utilize a computer to get access to private client information, business secrets, public data, or even take down a system (Dayanand 2020).

The term "hacking" was first used maliciously in the 1970s, when early computers phones were starting to become targets (Readway, 2017). Tech-savvy people known as "pneakers" have figured out a method to pay for long distance calls using a sequence of numbers. They were the first hackers to figure out how to manipulate the hardware and software of the gadget to steal long-distance phone time (Treadway, 2017). People learned from this that hostile behavior could compromise computer networks, and that the more advanced a system was, the more susceptible it was to cybercrime (Treadway, 2017).

Fast-forward to 1990, when the enormous project known as Operation Sun Devil was revealed. FBI agents confiscated 42 computers and more than 20,000 floppy disks that the suspects had been using to access credit cards and phone networks without authorization (Garcia, 2018). Only a small number of the offenders were found after two years of inquiry by about 100 FBI agents. However, it was seen as a wonderful public awareness effort since it was a means to show hackers that they will be identified and punished (Garcia, 2018). The Electronic Frontier Foundation was founded in response to threats to the public's rights that emerge when law enforcement commits mistakes or overinvests in its investigations into cybercrime.

Their goal was to defend and shield clients from legal action (Тігаренко, 2019). Even with the criminal justice system in place, crime and cybercrime continue to be major problems in our community. Both on the open internet and the dark web, cybercriminals are highly skilled and difficult to find (Huey, Nhan & Broll, 2013).

2.1.4 Cyber security cost and bank performance

The purpose of the study was to ascertain how satisfied Nigerian bank e-services' cybercrime victims were (Bamrara et al, 2012). The findings demonstrated a negative correlation between the type of bank and the provision of financial security and confidentiality as well as the high reliability of the current systems, while a positive correlation was found between the type of bank and the attribute of good public credibility, which also improves the financial performance of e-banks (Bamrara et al., 2012). The University of Nova Southeastern carried out the research on IT security for online banking. The findings indicated that investors paid more for information system security technologies than e-banking firms that made investment announcements based on information system security personnel, and they also revealed statistically significant market reactions for e-banking firms making information system security investment announcements (Brock & Levy, 2013). The researcher also identified the study gap since earlier empirical studies that used accounting-based indicators to examine the relationship between information system and firm performance had inconsistent results. Furthermore, a small sample size and stock market incidence also contribute to the research discrepancy (Brock & Levy, 2013).

The adoption of e-banking was the subject of an empirical study carried out in Cameroon. The study's findings showed that consumer adoption of e-banking is significantly influenced by perceived security, trust, service cost, usefulness, and accessibility, all of which have an impact on the financial performance of e-banking (Fonchamnyo, 2013). Reasoned action theory and planned behavior theory served as the research's theoretical cornerstones. The researcher also identified a study gap since it is important to identify the variables that prevent e-banking from being adopted and spread as well as those that may affect consumers' perceptions or attitudes toward e-banking adoption (Fonchamnyo, 2013). In Nigeria, more study was done on the use of online banking. According to Mehmood et al. (2014), the findings indicate that expenses related to privacy and security, website design, and trust greatly influence the use of e-banking, which in turn impacts the financial success

of e-banking in Nigeria. The notion of reasoned action and planned conduct served as the research's theoretical cornerstones. The researcher also drew attention to the gap, noting that Pakistan has conducted very few e-banking studies (Mehmood, et al., 2014).

The study on cybercrime and its impact on market return was carried out in Italy. The research discovered that stock market returns are impacted by news of cyberattacks, and that this is because public statements about cyberattacks often result in a negative reaction on the stock market (Arcuri et al., 2014). Researchers discovered, in particular, evidence of a general negative effect on the stock market to disclosures of breaches in information security. The study gap was identified by the researchers since there is little literature on cybercrime or information security breaches relating to the banking industry (Arcuri, et al., 2017).

Zimbabwe was the site of the banking industry's electronic fraud risk study (Dzomira, 2014). The findings indicate that the banking industry is involved in a number of the electronic fraud types mentioned. The investigation came to the conclusion that there are significant worries over the lack of funds to keep up with emerging technology as well as the ignorance of cyber crime (Dzomira, 2014). The lack of technology and resources for identifying computer crime and skilled investigators to carry out investigations also contributed to the establishment of the digital forensic threat. The researchers proposed the gap as they could not locate any studies that addressed cyber fraud specifically or the challenges that financial institutions confront in trying to combat this type of threat (Dzomira, 2014).

2.2 Theoretical Framework

2.2.1 Reasoned Action

The study's theoretical foundation is the reasoned action theory, which was created by (Ajzen & Fishbein, 1969). This theory seeks to make sense of the relationship between attitudes and actions in human behavior. Its main application is in behavior prediction, based on the goals and past behaviors of the individual. An individual's choice to engage in a specific activity is determined by the outcomes they hope to get by carrying out the behavior.

The main objective of reasoned action theory (TRA) is to provide an explanation for an individual's voluntary behaviors by examining the underlying motive that drives an action (Doswell et al., 2011). According to the TRA, an individual's motivation for engaging in a behavior is the main indicator of whether they will do so or not (Montano

& Kasprzyk, 2015). Furthermore, the normative dimension, which pertains to the societal standards around the behavior, also denotes if the activity is genuinely executed by the person or not. The idea states that the intention behind an action comes before the actual conduct (Ajzen & Madden, 1986). This kind of intention, referred to as behavioral intention, stems from the hope that carrying out the action would produce a certain outcome. The idea revolves around behavioral intention, which is determined by attitudes toward acts and subjective standards (Colman, 2015). According to the idea of reasoned action, having stronger motivations leads to more efforts to carry out the activity, which raises the likelihood that the conduct will be carried out.

2.2.1 Technology Acceptance Model

A theory of information systems called the Technology Acceptance Model (TAM) simulates how customers embrace and use new technologies. One of the most well-known applications of Ajzen and Fishbein's theory of reasoned action (TRA) in literature is the TAM. The most widely used model of consumer technology adoption and utilization is Davis's (Davis, 1989; Davis, Bagozzi, & Warshaw, 1989) technology acceptance model (Venkatesh, 2000). It was made by Richard Bagozzi and Fred Davis (Davis 1989; Bagozzi, Davis & Warshaw 1992). The TAM combines the ease of use and practicality of the two application recognition indicators with a large portion of the mindset indicators found in the Theory of Reasoned Actions (TRAs). The TRA and TAM, which both have distinct behavioral components, hold that they should be free to act whenever someone expresses a desire to do so. In the current world, there would be limitations, such a restricted right to function (Bagozzi, Davis & Warshaw, 1992).

2.3 Empirical Review

Okoro, Nnam, Joe and Obizuo (2024) examined the impact of financial technology on financial institutions' performance. Evidence from Nigerian banks. The volume of ATM transactions, POS transactions and internet bank transactions were used to measure financial technology while liquidity ratio was used to measure financial performance. To achieve the objective of the study, ex-post facto was adopted. The data were collected through secondary source from CBN statistical bulletin. The data collected were analyzed using ordinary least multiple regression analysis. The result revealed that ATM transactions have positive impact on the performance of commercial banks in Nigeria. POS transactions have positive impact on the performance of commercial banks in Nigeria.

Internet banking transactions have negative impact on the performance of commercial banks in Nigeria. In order to support the findings, the study recommends that financial institutions do more to entice their clients to use FINTECH products more regularly. This might be done through streamlining product usage, upholding product security, and guaranteeing product speed and efficiency.

Al-Somali, Saqr, Asiri, Al-Somali (2024) explored the impact of organizational cybersecurity systems on organizational resilience and sustainable business performance in Saudi Arabia's service and manufacturing sectors, examining the mediating and moderating effects of organizational resilience and culture. A quantitative research method was employed, combining a thorough literature review with empirical data from a sample of 394 respondents in Saudi Arabia, split evenly between the service and manufacturing sectors. Smart PLS 3.3.3 was used to test the proposed hypotheses. The findings suggested a positive effect of the factors of organizational cyber security systems on organizational resilience. Organizational cyber security systems also significantly influenced sustainable business performance; however, organizational resilience and culture did not play mediating and moderating roles. This study is one of the first to offer a nuanced analysis of IT capabilities and cybersecurity within Saudi Arabia's service and manufacturing sectors, especially in a post-COVID-19 context. The insights gleaned contribute to the academic discourse and have pivotal managerial implications for organizations navigating the digital era in Saudi Arabia.

Alejandra and Gustavo (2023) explored the connection between a firm's cybersecurity management practices and the probability of a cyber event occurring. This study also examines the financial impact of these events by analyzing losses recorded over the 12-month period following a cybersecurity incident, and its potential effect on credit risk. The findings demonstrate a strong relationship between the quality of cybersecurity practices and the probability of a reported cybersecurity event. Certain industries, such as Finance, Healthcare, and Technology exhibit relatively higher risk of cyber related financial losses. Likewise, larger companies face an elevated risk of security events compared to smaller ones. This study also illustrates the significant negative effects of cyber incidents on firm value, with severe events leading to persistent negative equity returns over a 12-month period. The findings demonstrate the potentially material financial implications of cyber risk, and highlight the importance of cybersecurity in a complete integrated risk

assessment framework

Aaron and Moti (2022) examined The Influence of Cyber Security Implementation Strategy on Organizational Knowledge Management and Performance. A conceptual model of knowledge management processes showing the relationship of knowledge acquisition, knowledge sharing, knowledge utilization and security compliance and its subsequent impact on organizational performance is proposed. The model is tested using data collected from a case study organization in Ghana. The study used structured questionnaires (open and close-ended questions) to collect data. The findings were coded into excel and analyzed using the SPSS software. It was established that organisational knowledge management has an influence on organizational performance.

Rufus, Olubunmi, Modupe and Abimbola (2022) carried out a study on cyber security and financial innovation of listed deposit money banks in Nigeria. The study adopted a survey research design with primary data obtained via a structured questionnaire administered to a sample size of fifty-six (56) Deposit Money Banks Staff purposively selected. The sampled staffs were senior member staff of key impacted departments while the Banks selected accounted for 93% of total market capitalization as on December 31, 2021. The primary data collected were analyzed using descriptive and inferential statistics. The study found that cyber security proxied by risk management and bank monitoring had a statistically and positively significant impact on financial innovation of deposit money banks in Nigeria ($Adj.R2 = 0.447$, $F(2,55)=23.274$, $p < 0.05$). It recommended that deposit money banks should ensure regular review, revision and strengthening of their risk management framework to meet with emerging challenges from the deployment of financial innovative products and services. Additionally, deposit money banks should improve on the level of monitoring of the deployed e-banking channels (Card products, POS, ATMs and other channels) to facilitate greater reliance on them for the consummation of financial transactions.

Khalid, Abid and Sheikh (2022) examine the effect of Cyber Security Costs on Performance of E-banking in Pakistan. The targeted population was a managerial cadre staff member of e-banks working in Pakistan. The data were collected using structured questionnaire. The data collected were analyzed using multiple regression analysis. The consequence exhibited that the cyber security costs put considerable influence on product innovation performance and e-banking financial performance and product innovation performance considerably

mediates in an association with cyber security costs and e-banking financial performance. The study concluded that the introduction of emerging technology and creative services and products has obviously had a positive effect on banks' operations. The recommendations and future area are also included in the study.

III. METHODOLOGY

3.1 Research Design

The research design adopted in this study is *ex-post facto* research design. This design was used because the researcher has no control over the exogenous variable and whatever happens occurred before the research. Furthermore, *ex-post facto* design was used when researchers are trying to ascertain the cause and effect of the relationships that exist between two variables.

3.2 Sources of data

Secondary source of data was adopted through the use of annual reports and statement of accounts of the selected deposit money banks for the period of the study (2014 – 2023) to generate data.

3.3 Population of the study

The population of this study is made up of all the fifteen (14) deposit money banks listed in Nigeria Exchange Group as at December, 2022. They include; Access Bank Plc, Eco Bank of Nigeria, Fidelity Bank Plc, First Bank of Nigeria, First City Monument Bank, Guaranty Trust Bank, Stanbic IBTC Bank, Sterling Bank Plc, Union Bank of Nigeria Plc, United Bank for Africa Plc, Unity Bank Plc, Wema Bank Plc, Zenith Bank Plc and Jaiz bank.

3.4 Sample size/sampling techniques of the study

The study adopted purposive sampling technique. The purposive sampling was used to selected only deposit money banks that have complete data on cyber security cost. It is unfortunate that some banks did not report their cost attributed to cyber security. Based on that, ten (10) deposit money banks were purposively selected as the sample size of the study. These deposit money are; Access Bank Plc, Eco bank, Fidelity Bank Plc, First Bank of Nigeria, First

4.2.1 Descriptive Statistics

Table 4.1: Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
CSC	100	3.07	8.29	5.7262	1.61550
ROA	100	.00	.25	.0366	.04937
ROE	100	.00	.37	.1276	.08539
EPS	100	-.03	6.05	1.2924	1.32538
Valid N (listwise)	100				

Source: Appendix 1

City Monument Bank, Guaranty Trust Bank, Stanbic IBTC Bank, Sterling Bank Plc, United Bank for Africa Plc, and Union bank Plc. The study was carried out for the period of 10 years ranging from 2014-2023.

3.5 Data Analysis Techniques

This study employed the Ordinary Least Square based simple regression model to understand the interaction among the variables and estimating the relevant data.

3.6 Model Specification

Khalid, et al (2021) model will be adopted by this study.

$$FP = \beta_0 + \beta_1PDC_{it} + \beta_2RC_{it} + \beta_3DC_{it} + \beta_4IC_{it} + e_i \dots \dots \dots \text{eq1}$$

The model was modified to suit the present objectives

$$ROA_{it} = \beta_0 + \beta_1CSC_{it} + e_i \dots \dots \dots \text{model 1}$$

$$ROE_{it} = \beta_0 + \beta_1CSC_{it} + e_i \dots \dots \dots \text{model 2}$$

$$EPS_{it} = \beta_0 + \beta_1CSC_{it} + e_i \dots \dots \dots \text{model 3.}$$

Where;

CSC = Cyber security cost

ROA = Return on asset

ROE = Return on equity

EPS = Earnings per share

e = error term signifying other variables not captured in the study

_{it} = Firm i at time t

IV. DATA ANALYSIS, RESULT AND DISCUSSIONS

4.1 Data Presentation

The analysis focused on cyber security cost and financial performance of listed Deposit Money Banks in Nigeria. Cyber security cost (CSC) represents the independent variable of the study and was measured using cost associated to technologies and e-businesses. However, financial performance represents the dependent variable of the study and it was measured using return on asset (ROA), return on equity (ROE) and earnings per share (EPS).

4.2 Data Analysis.

The data were analysed using both descriptive statistics and multiple regression analysis.

Table 4.1 shows that descriptive statistics of the variables. The result showed that cyber security cost (CSC) has the minimum of 3.07 and maximum of 8.29. Return on asset (ROA) has the minimum 0.00 and maximum of 0.25. return on equity (ROE) has the minimum of 0.000 and maximum of 0.37. while earnings per share (EPS) has the minimum of -0.03 and maximum of 6.05. It is also revealed that the mean values of CSC, ROA, ROE and EPS are 5.7262, 0.0366, 0.1276 and 1.2924 respectively for the period covered by the

study, indicating that the average value of CSC of the series is 5.7%, ROA is 0.0366%, that of ROE is 0.1276% and EPS is 1.2924%.

The standard deviation (Std. Dev.) indicates the dispersion from or spread of the series from their mean values. CSC has the highest dispersion of 1.61550, followed by reporting EPS with the dispersion of 1.32538. ROE has a dispersion of 0.8539 while ROA has the lowest dispersion of 0.04937.

4.2 Regression Analysis

Parameters	Model 1 (ROA)	Model 2 (ROE)	Model 3 (EPS)
Constant	0.068167	0.013069	-0.047217
Coefficient	-0.005440	0.020229	0.236330
Std Error	0.003043	0.004889	0.079329
T-statistics	-1.787798	4.137950	2.979100
R-Square	0.031900	0.150037	0.083826
Adjusted R-Square	0.021919	0.141275	0.074381
F-statistics	3.196221	17.12263	8.875039
P-value	0.076931	0.000075	0.003653

Source: Appendix 2A, 2B and 2C

Table 4.3, presents the regression result on the effect of cyber security cost (CSC) on financial performance (ROA, ROE and EPS). From the model summary table above, the following information can be distilled.

Empirical analysis for model 1

The R^2 which measure the level of variation of the dependent variable caused by the independent variables stood at 0.0319. The R^2 otherwise known as the coefficient of determination shows the percentage of the total variation of the dependent variable (ROA) that can be explained by the independent or explanatory variable (CSC). Thus the R^2 value of approximately 0.032 indicates that 3.2% of the variation in the ROA of deposit money banks can be explained by a variation in cyber security cost while the remaining 97.8% (i.e. $100-R^2$) could be accounted by other factors not included in this model.

The regression result as presented in table 4.2 determines the relationship between CSC and ROA shows that when all the independent variables are held stationary; the ROA variable is estimated at 0.068. This simply implies that when all independent variables are held constant, there will be an increase in the ROA of deposit money banks up to the tune of 0.068% occasioned by factors not incorporated in this study. Thus, a unit increase in CSC will lead to a decrease in ROA by 0.005440%. Finally, the result shows that there is a significant variation of Fisher's statistics (3.19622) has the

probability value of 0.076931 which means the model as a whole is not statistically significant at 5% level.

Empirical analysis for model 2

The R^2 which measure the level of variation of the dependent variable caused by the independent variables stood at 0.150037. The R^2 otherwise known as the coefficient of determination shows the percentage of the total variation of the dependent variable (ROE) that can be explained by the independent or explanatory variable (CSC). Thus the R^2 value of approximately 0.150 indicates that 15.0% of the variation in the ROE of deposit money banks can be explained by a variation in cyber security cost while the remaining 85.0% (i.e. $100-R^2$) could be accounted by other factors not included in this model.

The regression result as presented in table 4.2 determines the relationship between CSC and ROE shows that when all the independent variables are held stationary; the ROE variable is estimated at 0.013069. This simply implies that when all independent variables are held constant, there will be an increase in the ROE of deposit money banks up to the tune of 0.013069% occasioned by factors not incorporated in this study. Thus, a unit increase in CSC will lead to a decrease in ROE by 0.020229%. Finally, the result shows that there is a significant variation of Fisher's statistics (17.12263) has the probability value of 0.000075 which means the model as a whole is statistically significant at

5% level.

Empirical analysis for model 3

The R^2 which measure the level of variation of the dependent variable caused by the independent variables stood at 0.083826. The R^2 otherwise known as the coefficient of determination shows the percentage of the total variation of the dependent variable (EPS) that can be explained by the independent or explanatory variable (CSC). Thus the R^2 value of approximately 0.084 indicates that 8.4% of the variation in the EPS of deposit money banks can be explained by a variation in cyber security cost while the remaining 91.6% (i.e. $100-R^2$) could be accounted by other factors not included in this model.

The regression result as presented in table 4.2 determines the relationship between CSC and EPS shows that when all the independent variables are held stationary; the EPS variable is estimated at -0.047217. This simply implies that when all independent variables are held constant, there will be an increase in the EPS of deposit money banks up to the tune of 0.047217% occasioned by factors not incorporated in this study. Thus, a unit increase in CSC will lead to a decrease in EPS by 0.236330%. Finally, the result shows that there is a significant variation of Fisher's statistics (8.875039) has the probability value of 0.003653 which means the model as a whole is statistically significant at 5% level.

4.3 TEST OF HYPOTHESIS

Hypothesis one

HO₁: Cyber security cost has no significant effect on return on asset of listed deposit money banks in Nigeria.

Since the calculated probability value 0.076931 is greater than the accepted probability value of 0.05. The null hypothesis is accepted and the alternative rejected thus; Cyber security cost has no significant effect on return on asset of listed deposit money banks in Nigeria.

Hypothesis two

HO₂: Cyber security cost has no significant effect on return on equity of listed deposit money banks in Nigeria.

Since the calculated probability value 0.000075 is less than the accepted probability value of 0.05. The null hypothesis is rejected and the alternative accepted thus; Cyber security cost has a significant effect on return on equity of listed deposit money banks in Nigeria.

Hypothesis three

HO₂: Cyber security cost has no significant effect on earnings per share of listed deposit money banks in Nigeria.

Since the calculated probability value 0.003653 is less than the accepted probability value of 0.05. The null hypothesis is rejected and the alternative accepted thus; Cyber security cost has a significant effect on earnings per share of listed deposit money banks in Nigeria.

4.4 DISCUSSIONS ON FINDINGS

The result of hypothesis one revealed that Cyber security cost has no significant effect on return on asset of listed deposit money banks in Nigeria. The result is contrary with prior studies of Al-Somali, et al. (2024), which explored the impact of organizational cybersecurity systems on organizational resilience and sustainable business performance in Saudi Arabia's service and manufacturing sectors, examining the mediating and moderating effects of organizational resilience and culture. The findings suggested a positive effect of the factors of organizational cyber security systems on organizational resilience. Organizational cyber security systems also significantly influenced sustainable business performance; however, organizational resilience and culture did not play mediating and moderating roles. Consequently, the result is contrary with prior studies of Khalid, et al. (2022), which examine the effect of Cyber Security Costs on Performance of E-banking in Pakistan. The data were collected using structured questionnaire. The data collected were analyzed using multiple regression analysis. The consequence exhibited that the cyber security costs put considerable influence on product innovation performance and e-banking financial performance and product innovation performance

The result of hypotheses 2 and 3 revealed that cyber security cost has a significant effect on return on equity and earnings per share of listed deposit money banks in Nigeria. The findings is consistent to the findings of Rufus, et al (2022), which examined impact of cyber security in driving the financial innovation of Deposit Money Banks in Nigeria. The study found that cyber security proxied by risk management and bank monitoring had a statistically and positively significant impact on financial innovation of deposit money banks in Nigeria (Adj. $R^2=0.447$, $F_{(2,55)}=23.274$, $p<0.05$). Also, Khalid, et al. (2021), examined impact of cyber security cost on the financial performance of e-banking: mediating influence of product innovation performance. The survey was conducted by distributing the questionnaire among the employees of e-banks working in Pakistan. The

collected data were estimated via multivariate statistical techniques. The results of the study showed that a) the costs associated with cybersecurity, specifically PDC, RC, and DC, have a statistically significant effect on PIP and e-banking FP, whereas IC has a negative significant influence on the PIP and FP, b) the PIP has a statistically significant effect on e-banking FP, and c) the PIP partially mediates an association between PDC, RC, DC, and FP, whereas, PIP insignificantly mediates in a relationship amongst IC and e-banking FP.

V. CONCLUSION AND RECOMMENDATIONS

5.1 Summary of Findings

The following findings were summarized thus:

- (i) Cyber security cost has no significant effect on return on asset of listed deposit money banks in Nigeria.
- (ii) Cyber security cost has a significant effect on return on equity of listed deposit money banks in Nigeria.
- (iii) Cyber security cost has a significant effect on earnings per share of listed deposit money banks in Nigeria.

5.2 Conclusion

The analysis focused on cyber security cost and financial performance of listed deposit money banks in Nigeria. Data were collected from annual report and account of the 10 selected banks for the period of 10 years ranging from 2014 to 2023. The data collected were analyzed using both descriptive and inferential statistics (multiple regression analysis). The findings revealed that cyber security cost has a significant effect on return on equity and earnings per share but does not have significant effect on return on asset of listed deposit money banks in Nigeria. Based on level of significance, it can be concluded that cyber security significantly affect bank performance in Nigeria.

5.3 Recommendations

Based on the findings of this study, it is therefore recommended that:

- (i) It is recommended that the banks take more cost-effective steps and more reliable technologies that do not offer loopholes for illegal activities to take place. There should also be more investment in prevention and detection techniques, because banks invest significant sums in the production of these goods. The cost incurred in providing this security should accounted and reported in the financial

statement to guide investors on true nature of the company especially in the area of their return on asset.

- (ii) The study found that the aftermath of a cyber-attack is marked by the effect of a variety of stakeholders, not just the bank. The study advises that banks should enter into insurance cover arrangements with other financial institutions to include insurance coverage for some of the expenses incurred by banks in order to avoid a decrease in operations, causing the loss of profit. This will help in increasing the return on equity of deposit money banks in Nigeria.
- (iii) Proper creation of the cyber security may protect individuals from cyber-attacks. Cyber security providers at this level much work hard to provide better security to the customers. In addition, organizations and service providers can also provide tailored security training to the banks customers or users when they need it. Also, the cost incurred in providing this security should be accurately reported in the financial statement to guide investors on true nature of the company especially in the area of their earnings per share.

REFERENCES

- [1]. Aaron, R. & Moti, Z. (2022). The Influence of Cyber Security Implementation Strategy on Organizational Knowledge Management and Performance. *Journal of Management*, 35(3), 217-228.
- [2]. Agwu, E., & Carter, A. L. (2014). Mobile phone banking in Nigeria: benefits, problems and prospects. *International Journal of Business and Commerce*, 3(6), 50-70.
- [3]. Ahmed, Q. M. M. (2018). Analysis of the recent attacks on Pakistani Banks. PakCERT Threat Intelligence Report. 1(3), 20-34.
- [4]. Ajzen, I., & Fishbein, M. (1969). The prediction of behavioral intentions in a choice situation. *Journal of experimental social psychology*, 5(4), 400-416.
- [5]. Ajzen, I., & Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control. *Journal of experimental social psychology*, 22(5), 453-474.
- [6]. Alejandra and Gustavo (2023). The impact of

- cybersecurity management practices on the likelihood of cyber events and its effect on financial risk. Princeton University Press, Princeton, NJ, 2023.
- [7]. Al-Somali, S.A.; Saqr, R.R.; Asiri, A.M.; & Al-Somali, N.A. (2024). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *Sustainability* 2024, 16, 1880.
- [8]. Aral, S., & Weill, P. (2007). IT assets, organizational capabilities, and firm performance: How resource allocations and organizational differences explain performance variation. *Organization science*, 18(5), 763-780.
- [9]. Arcuri, M. C., Brogi, M., & Gandolfi, G. (2017). The effect of information security breaches on stock returns: Is the cyber crime a threat to firms?. In *European Financial Management Meeting*.
- [10]. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber Security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.
- [11]. Bagozzi, R. P., Davis, F. D., & Warshaw, P. R. (1992). Development and test of a theory of technological learning and usage. *Human relations*, 45(7), 659-686.
- [12]. Bamrara, D., Chouhan, G. S., & Bhatt, M. (2012). An Explorative Study of Satisfaction Level of Cyber-crime Victims with Respect to E-services of Banks. *Journal of Internet Banking and Commerce*, 17(3).
- [13]. Beck, T., Chen, T., Lin, C. & Song, F.M. (2014). "Financial Innovation: The Bright and the Dark sides." *Journal of Banking and Finance*. 72 (C), 28-51, 2014.
- [14]. Bogati, D., & Vongurai, R. (2018). Determinants Of Customer Satisfaction And Customer Loyalty In E-Banking: A Case Study of Thailand's Selected Commercial Banks in Bangkok's Central Business Area. *International Research E-Journal on Business and Economics*, 2(2), 32.
- [15]. Bose,R.,& Luo,X.R.(2014). Investigating security investment impact on firm performance. *International Journal of Accounting & Information Management*, 22(3), 194-208.
- [16]. Brock, L., & Levy, Y. (2013). The market value of information system (IS) security for e-banking. *Online Journal of Applied Knowledge Management (OJAKM)*, 1(1), 1-17.
- [17]. CBN. (2017). Cyber security for Deposit Money Banks (DMBs) and Payment Service Providers' (PSPs). *Quarterly Economic Review*, pp 35-56, 2017.
- [18]. Chiu, C. L., Chiu, J. L., & Mansumittrchai, S. (2019). Stages in the development of consumers' online trust as mediating variable in online banking system: a proposed model. *International Journal of Electronic Finance*, 9(3), 170-201.
- [19]. Chong, A. Y. L., Ooi, K. B., Lin, B., & Tan, B. I. (2010). Online banking adoption: an empirical analysis. *International Journal of bank marketing*.
- [20]. Colman, A. (2015). Theory of reasoned action. *A Dictionary of Psychology*, 4.
- [21]. Columbus, L. (2020). Top 10 Cyber Security companies to watch in 2020. <https://www.forbes.com/sites/louisacolumbus/2020/01/26/top-10-CyberSecurity-companies-to-watch-in-2020/#3d820fd24fe6>
- [22]. Cui, M., Wang, J., & Yue, M. (2019). Machine Learning-Based Anomaly Detection for Load Forecasting Under Cyberattacks. *IEEE Transactions on Smart Grid*, 10(5), 5724-5734.
- [23]. Daniel, E. (1999). Provision of electronic banking in the UK and the Republic of Ireland. *International Journal of bank marketing*.
- [24]. Davis, F.D., Bagozzi, R.P., & Warshaw, P.R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science*, 35(8), 982-1003.
- [25]. Dayanand, D. G. B. (2020). Cybercrime an escalating and antisocial act: Types and Preventive Measures. *Studies in Indian Place Names*, 40(42), 228-233.
- [26]. Desta, Y. (2018). Customers' e-banking adoption in Ethiopia, PhD Dissertation, Addis Ababa University, Ethiopia.
- [27]. Devaraj, S., & Kohli, R. (2000). Information technology payoff in the health-care industry: a longitudinal study. *Journal of management information systems*, 16(4), 41-67.
- [28]. Doswell, W. M., Braxter, B. J., Cha, E., & Kim, K. H. (2011). Testing the theory of reasoned action in explaining sexual behavior among African American young teen girls. *Journal of pediatric nursing*, 26(6), e45-e54.
- [29]. Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, 4(2), 16-

- 26.
- [30]. Faems, D., De Visser, M., Andries, P., & Van Looy, B. (2010). Technology alliance portfolios and financial performance: value-enhancing and cost-increasing effects of open innovation. *Journal of Product Innovation Management*, 27(6), 785-796.
- [31]. Fianyi, I., D. (2015). Curbing cybercrime and enhancing e-commerce security with digital forensics, *International Journal of Computer Science Issues*, 12(6), 78-92.
- [32]. Fonchamnyo, D. C. (2013). Customers' perception of E-banking adoption in Cameroon: An empirical assessment of an extended TAM. *International Journal of Economics and Finance*, 5(1), 166-176.
- [33]. Garcia, N. (2018). The use of criminal profiling in cybercrime investigations (Doctoral dissertation, Utica College).
- [34]. Governance, C. (2019). Corporate Governance and Financial Performance Of Nigerian Banks– PDF–Complete Project Material. Accounting & Finance.
- [35]. Gupta, M. (2019). A Study of Customer Awareness Towards Internet Banking. *Advance and Innovative Research*, 86.
- [36]. Haq, Q. A. U. (2019). Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan. *International Journal of Computer Network and Information Security*, 11(1), 62.
- [37]. Henri, J. F., & Wouters, M. (2019). Interdependence of management control practices for product innovation: The influence of environmental unpredictability. *Accounting, Organizations and Society*, 101073.
- [38]. Huey, L., Nhan, J., & Broll, R. (2013). 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice*, 13(1), 81-97.
- [39]. Islam, S., Kabir, M. R., Dovash, R. H., Nafee, S. E., & Saha, S. (2019). Impact of Online Banking Adoption on Bank's Profitability: Evidence from Bangladesh. *European Journal of Business and Management Research*, 4(3).
- [40]. Jepchumba, P., & Simiyu, E. (2019). Electronic Banking Adoption and Financial Performance of Commercial Banks in Kenya, Nairobi City County. *International Journal of Finance and Accounting*, 4(2), 19-38.
- [41]. Kashmari, A., Ahg, N., & Nayebyazdi, A. (2016). "Impact of Electronic Banking Innovations on Bank Deposit Market Share." *The Journal of Internet Banking and Commerce*, 21(1), 1-5, 2016.
- [42]. Khalid, K. Abid, U. & Sheikh, R. (2022). Effect of Cyber Security Costs on Performance of E-banking in Pakistan. *International Journal of Innovation*, 17(1), 582-594.
- [43]. Khalid, K. Sheikh, R. Muhammad, T. Nisar, K. & Khalid, J. (2021). Impact of cyber security cost on the financial performance of e-banking: mediating influence of product innovation performance. *Journal of Humanities & Social Sciences Reviews*.
- [44]. Khari, M., Shrivastava, G., Gupta, S., & Gupta, R. (2017). Role of Cyber Security in Today's Scenario. In *Detecting and Mitigating Robotic Cyber Security Risks* (pp. 177-191). IGI Global.
- [45]. Mahmoud, M. A. (2019). Gender, E-Banking, and Customer Retention. *Journal of Global Marketing*, 32(4), 269-287.
- [46]. Malik, J.K., & Choudhury, S. (2019). A Brief review on Cyber Crime-Growth and Evolution. *Pramana Research Journal*, 9(3), 242.
- [47]. Mehmood, N., Shah, F., Azhar, M., & Rasheed, A. (2014). The factors effecting e-banking usage in Pakistan. *Journal of Management Information System and E-commerce*, 1(1), 57-94.
- [48]. Menon, N. M., & Lee, B. (2000). Cost control and production performance enhancement by IT investment and regulation changes: evidence from the healthcare industry. *Decision Support Systems*, 30(2), 153-169.
- [49]. Montano, D. E., & Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health behavior: Theory, research and practice*, 70(4), 231.
- [50]. Najaf, R., Najaf, K., & Pasowal, B. A. (2014). E-banking in Pakistan. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, 10(1), 74-84.
- [51]. Nazaritehrani, A., & Mashali, B. (2020). Development of E-banking channels and market share in developing countries. *Financial Innovation*, 6(1), 12.
- [52]. Njoroge, E. W. (2017). Effect of Cyber Security related costs on development of product innovation performances and services: A case study of NIC bank of Kenya. PhD Dissertation. Kenyatta University of

- Agriculture and Technology.
- [53]. Njoroge, E., & Njeru, A. (2017). The Effect of Cyber-Crime Response Costs on the Development of Financial Products: A Case of NIC Bank of Kenya.
- [54]. Nurse, J. R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624.
- [55]. Odhiambo, S. O., & Ngaba, D. (2019). E-banking services and financial performance of commercial banks in Kenya. *International Academic Journal of Economics and Finance*, 3(4), 132-153.
- [56]. Ojeka, S. & Egbide, B. (2017). "Cybersecurity in the Nigerian banking sector." *International Review of Management and Marketing*, 7(2), 340-346, 2017.
- [57]. Okechi, O., & Kepeghom, O. M. (2013). Empirical evaluation of customers' use of electronic banking systems in Nigeria. *African Journal of Computing & ICT*, 6(1), 7-20.
- [58]. Okoro, C.C. Nnam, H.I. Joe, W.E. & Obizuo, C.J. (2024). impact of financial technology on financial institutions' performance. Evidence from Nigerian banks. *International Journal of Accounting and Financial Management Research*, 10(3), 111-134.
- [59]. Padmaavathy, P. A. (2019). Cyber Crimes: A Threat To The Banking Industry. *International Journal of Management Research and Reviews*, 9(4), 1-9.
- [60]. Rathore, M. M., Paul, A., Hong, W. H., Seo, H., Awan, I., & Saeed, S. (2018). Exploiting IoT and big data analytics: Defining smart digital city using real-time urban data. *Sustainable cities and society*, 40, 600-610.
- [61]. Rathore, N. (2016). Ethical hacking & security against cyber crime. *Research Gate*, 15 (1), 26- 38.
- [62]. Rufus, Olubunmi, Modupe & Abimbola (2022). Cyber security and financial innovation of listed deposit money banks in Nigeria. *Universal Journal of Accounting and Finance*, 10(3) :643-652
- [63]. Shaari, R. (2020). Internet banking: from the perspective of Malaysian bankers. *International Journal of Management Studies*, 12(2), 115-124.
- [64]. Sheth A., Bhosale S., Kurupkar F. (2021). "Research Paper on Cybersecurity." *Contemporary Research in India Journal*. 4(1), 246-251.
- [65]. Siddik, M. N. A., Sun, G., Kabiraj, S., Shanmugan, J., & Yanjuan, C. (2016). Impacts of e- banking on performance of banks in a developing economy: empirical evidence from Bangladesh. *Journal of Business Economics and Management*, 17(6), 1066-1080.
- [66]. Solms R.V., Niekerk G.J.U. (2013). From information security to cybersecurity. *Computers and Society Journal*. 38(1), 97-102, 2013
- [67]. Söylemez, S. A., & Ahmed, A. H. (2019). The Role of New Economy Indicators on Banking Sector Performance in Ghana: Trend and Empirical Research Analysis of Banks' Clients and Experts Perception. *Journal of Finance and Economics*, 7(1), 23-35.
- [68]. Strassmann, P. A. (1997). The squandered computer: evaluating the business alignment of information technologies. Strassmann, Inc..
- [69]. Thankgod, U. J., Alhassan, Y., & James, E. M. (2019). Effect Of Electronic Payment On Financial Performance Of Deposit Money Banks In Nigeria. *Lafia Journal Of Economics And Management Sciences*, 4(1), 114-114.
- [70]. Treadway, K. N. (2017). Comparing the Cognitive Abilities of Hackers and Non-Hackers Using a Self-Report Questionnaire (Doctoral dissertation, Purdue University).
- [71]. Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(4), 710-729.
- [72]. Usman, M. (2017). Cyber Crime: Pakistani Perspective. *Islamabad Law Review*, 1(3), 18-III.
- [73]. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46(2), 186-204.
- [74]. Wang, D., Xiang, Z., & Fesenmaier, D.R. (2016). Smart phone use in everyday life and travel. *Journal of Travel Research*, 55(1), 52-63.
- [75]. Yar, M., & Steinmetz, K.F. (2019). Cyber crime and society. SAGE Publications Limited.
- [76]. Zaid, A. H. A., Azman, N., & Azizan, N. (2020). Success Factors Consideration for E-banking Web site from User Perspectives in Malaysia: A Study Using the Knowledge Transfer Process Model. *Journal of Global Scientific Research* (ISSN: 2523-9376), 1,



295-306.