SPECTRUM
Journal of Social Sciences

ASPUR PUBLISHING

Vol. 03, No. 01 (2026) 25-42, doi: 10.61552/SJSS.2026.01.004 - http://spectrum.aspur.rs

CYBERSECURITY PRACTICES AND OPERATIONAL PERFORMANCE IN NIGERIAN BANKS

Abdulhameed Idris
Frank Alaba Ogedengbe[1]
Amal Altalhi

Received 17.10.2024.
Revised 11.01.2025.
Accepted 19.02.2025.

Keywords:

Cybersecurity, Operational Performance, Nigerian Banks, Risk Management, Regulatory Compliance, Fraud Prevention, Financial Stability.

Original research

A B S T R A C T

The increasing digitization of financial services has made cybersecurity a critical concern for banks worldwide, including in Nigeria. As cyber threats continue to evolve, banks must implement robust security measures to protect sensitive customer data, maintain trust, and ensure seamless operations. This study explores the relationship between cybersecurity practices and operational performance in Nigerian banks, focusing on risk management strategies, regulatory compliance, technological adoption, and fraud prevention mechanisms. Using a combination of qualitative and quantitative methods, the research examines how cybersecurity frameworks influence service efficiency, financial stability, and customer confidence. The findings reveal that banks with strong cybersecurity protocols experience improved operational resilience, reduced financial losses, and enhanced regulatory compliance. Furthermore, the study highlights the challenges faced by Nigerian banks in implementing effective cybersecurity measures, such as financial constraints, skill shortages, and evolving cyber threats. The research concludes by emphasizing the need for continuous investment in cybersecurity infrastructure, staff training, and policy enforcement to safeguard the banking sector against cyber risks and ensure sustainable growth.

1. INTRODUCTION

When banking institutions face cyber security threats, they can enter a systemic crisis capable of threatening the stability of the financial markets. Unexpected situations or serious threats can have a negative impact on the organizations, stakeholders, or the companies if not handled properly (Alketbi et al., 2022). Despite all the technological interventions that banks can deploy to deal with online security threats, technology alone is not enough to protect banks (Arachchilage & Love, 2014). Therefore, security measures should also include cultural, technical and behavioural interventions (Wada & Odulaja, 2012).

The increasing digitization of banking services in Nigeria has significantly transformed the financial sector, providing enhanced convenience and efficiency for customers. However, this rapid technological advancement has also exposed banks to sophisticated cyber threats, including data breaches, phishing attacks, and ransomware, which threaten the confidentiality, integrity, and availability of financial systems. Despite growing awareness of these risks, many Nigerian banks

[1] Corresponding author: Frank Alaba Ogedengbe
Email: ogedengbe@nileuniversity.edu.ng

continue to face challenges in implementing effective cybersecurity practices.

Insufficient investment in cybersecurity infrastructure, lack of skilled personnel, and inadequate regulatory compliance have left several banks vulnerable to attacks, resulting in financial losses, reputational damage, and decreased customer trust. Furthermore, there is limited empirical evidence linking the adoption of robust cybersecurity measures to improved operational performance, leaving a critical gap in understanding how these practices can enhance efficiency, reduce downtime, and safeguard assets.

This problem is aggravated by the dynamic nature of cyber threats and the varying levels of preparedness among banks, which create disparities in their ability to respond effectively. As cyber threats continue to evolve, there is an urgent need to assess the current state of cybersecurity practices in Nigerian banks and their impact on operational performance, providing actionable insights to strengthen resilience and foster sustainable growth in the sector. Against the backdrop, this study seeks to investigate the effect of cyber security of the operational performance of the Banking sector in Nigeria using UBA as a case study.

The major objective of this study is to investigate the impact of cyber security on the performance of UBA, Abuja. However, the specific objectives of this study include firstly, determining the effect of cloud security implementation on productivity of UBA in Abuja. Secondly it is to determine the effect of effective internal control implementation on productivity in UBA, Abuja. And thirdly to assess the effect of material security on productivity of UBA Abuja.

This study sets to test the following hypotheses in the process. Firstly, cloud security implementation has no significant effect on the productivity of UBA, Abuja. Secondly, the implementation of effective internal control has no significant effect on the productivity of UBA Abuja. And thirdly effective material safety has no significant effect on the productivity of UBA, Abuja.

2. LITERATURE REVIEW

The goal of cybersecurity is to defend against harmful assaults on computers, servers, mobile devices, electronic systems, networks, and data. Cybersecurity also refers to a set of plans and actions designed to protect personal and organizational data, information and networks against all threats that can be caused internally or externally (Solansky & Beck, 2021). These threats include unauthorized access and disclosure, misuse of data/information, cyber theft and organized attacks by exposing malware and other types of foreign viruses. According to Li and Liu (2021), network security measures can be broadly divided into five main categories: measures that focus on software security, network security, service security, cloud security, user training and information security. Elaborating further, these measures include the use of passwords and authentication procedures, firewalls and data encryption techniques, malware scanners and anti-virus software (Yousuf & Mir, 2019).

There is a common misinterpretation between cybersecurity and "information security." Akintoye et al. 2022 from the International Telecommunication Union state that the primary goal of cyber security is to guarantee the confidentiality, availability, and integrity of information in the appropriate quantities, to the appropriate individuals, and at the appropriate locations because this CIA Due to the attraction of data and information in the hands of the guards and the significant impact that their breach would have on the institution's activity, the third (Confidentiality, Integrity, Availability) is crucial for financial institutions that are banking institutions and economy in general. For instance, the Electronic Fraud Forum's 2020 report ("E-Fraud Forum of Nigeria") states that as of 2019, the total value of online fraud was over 6.1 billion naira. As a result, deposit banks can use this as a creative focal point to enhance the cyber security architecture through increased risk management and regular bank management in compliance with regulatory standards. The recommendations specifically stipulate that every bank must use suitable monitoring indicators and establish a "risk management plan to reduce the occurrence of adverse effects". Thus, to assess the cyber security performance of Nigerian commercial banks, the two aspects of risk management strategy and banking compliance will be used as representative indicators in this study.

According to Jacobson and Idziorek (2012), internet security is essentially the act of making sure websites are safe from both known and unexpected dangers. The artificial world produced by humans, which includes the Internet, social networks, computer networks and systems, and even intelligent software, is referred to as the "web" by Limnéll et al. (2015). The North Atlantic Treaty Organization (NATO) defines cyber security as a fundamental idea to safeguard national secrets and ensure national security (Klimburg, 2011a, Klimburg 2011b). The tools, policies, security concepts, security measures, regulations, and risk management used to safeguard the assets of businesses, organizations, and Internet of Things users are referred to as cyber security by the International Telecommunication Union (ITU) (2019). Other definitions include training, best practices, and technology. Understanding the problems associated with different cyberattacks and developing defensive tactics (accounting) that preserve the confidentiality, availability, and integrity of all digital systems and information are important to the field of cybersecurity (Muhati, 2018).

The international response to the growing challenges of cyber security to ensure a global information society where trust and security in the use of ICT are normal for the benefit of Humanity Global Cybersecurity Society (GCA), which provides a system that can be coordinated with. addressed (Kuerbis & Badiei, 2017). The GCA is an international cooperation framework that aims to

bring together all stakeholders, including governments, the private sector, civil society and international organizations, to build trust and security in the information society. GCA is based on five pillars with seven strategic objectives. The five pillars are legal measures, technical and strategic measures, organizational structure, capacity building, and international cooperation.

Legal measures are needed to establish national laws where they do not exist, and existing laws and regional and international agreements define what constitutes cybercrime and cyberattacks and how to deal with them must consider common understanding technical methods and procedures comply with international regulations. standards intended to provide a hardware and software foundation upon which vendors, software developers, and end users can demonstrate a need to identify and develop solutions. Features: This indicates the need to put in place appropriate institutional arrangements, such as national coordination and responsible response agencies, to quickly respond to cyber-attacks and coordinate with their counterparts at the international level. The last two pillars, capacity building and international cooperation, allow all disciplines and ensure that the necessary capacities are in place to enable IT security professionals to respond effectively in the event of cyber-attacks in the global economy and build relationships and cooperation at the international level (Kuerbis & Badiei, 2017).

Cybercrime security strategy is the joint implementation of security strategies, plans, threat management systems, specific measures and values that can be taken to protect information systems. (International Telecommunication Union, 2019). Cyber security is the security of the internet, computer networks, and the security of electronic systems (Adebiyi & Olayemi, 2022; Olaniran 2022). Preventing data loss and maintaining data integrity requires strong cybersecurity measures, including early detection, prevention, and the ability of systems to continue operating during and after an attack. These are important factors to consider when developing strategies to reduce the impact of cybercrime.

Kaspersky Lab ™ categorized network security as follows: (a) Network security protects computer networks from opportunistic malware and targeted attacks, among other intrusions. (b) Software security guards against attacks on both hardware and software. Malware can access data that it is meant to secure. Effective security begins well in advance of the system or gadget being put into use, at the design stage. (c) Data integrity and confidentiality, both in transit and at rest, are the focus of information security. (d) Data asset maintenance and protection policies and procedures are part of operational security. This category includes all measures to ascertain consumers' preferences about Internet access as well as the storage and sharing of data. (e) Disaster recovery and business continuity refers to an organization's procedures for handling events involving cyber security and other situations that cause a loss of data or services. The process by which an organization will return to its pre-event operating capabilities in terms of information and services is outlined in its disaster recovery plan. Organizations rely on the idea of business continuity when attempting to function without specific resources and end-user training that considers people—an unpredictable component of cybersecurity. Inadvertently introducing a virus into a secure system is possible for anyone who does not adhere to accepted security protocols. For the security of any firm, it is imperative that users learn how to delete dubious email attachments, avoid connecting in unrecognized USB drives, and many other crucial lessons.

Information security must be established and executed concurrently with the building of ICT infrastructure, since it is the driving force behind regional economic development. The advantages that come with deploying IT services are contingent upon the concurrent development of ICT infrastructure and a suitable legal and regulatory framework. The digital economy can thrive with strong regulations and appropriate security measures (Mohamed Abdel Razek Youssef, 2022). It takes a wide understanding of ICT security, including the legislative framework, to draw in players who have the means and the motivation to create a desirable business climate. This is the primary element that guarantees the profitability of infrastructure investments. Therefore, for developing nations that wish to engage in the global economy, cyber security instruments and the related legal framework provide greater challenges. A worldwide information society will steer clear of dangers like the creation of virtual paradises and the denial of users access to efficient digital security (Mohamed Abdel Razek Youssef, 2022).

2.1 Effect of Security Strategy on Banks' Profitability.

The banking sector is one of the most dangerous sectors because of the type of data it has (Shaker et al. 2023). This means that banks have had to invest a lot of money in the development of digital infrastructure to strengthen their cyber security (Shaker et al., 2023). The potential risks of online hacking, virus attacks and other information security breaches are increasing rapidly as we become more dependent on the Internet (Arachchilage & Love, 2014). Although banks in emerging countries are integrating security features, consumer behaviour creates security vulnerabilities (Ojeka et al., 2017). Many cyber security threats and vulnerabilities continue to exist worldwide (Mohamed Mizan et al., 2019).

It is not hyperbole to state that the banking sector was the primary representative and suffered the greatest amount of damage during the 2008 global recession (Hudson & Maioli, 2010). Between 2008 and 2012, 465 banks failed in the United States (Hudson & Maioli, 2010). 2019 saw the banking sector remain in decline as other industries began to recover. Concerns have been raised recently about the general performance of Greek banks in Greece. Greek banks' pre-disbursements and pre-tax profits are meagre. According to the chairman of Piraeus Bank, the

largest issue facing the Greek economy is the country's high percentage of non-performing loans, as CNBC reported (Congdon, 2022). This is a higher percentage than Italy's 9.7% (Congdon, 2022).

Of $23.4 billion in deposits as of September 2019, just $5 billion had been lent to individuals and the business sector in Africa, according to the Reserve Bank of Zimbabwe (RBZ). Based on Oni (2019) data, it can be inferred that the average loan-to-deposit ratio in the banking industry is a mere 24%, and it has been declining since 2015. In 2016, non-performing loans posed a serious threat to Zimbabwe's banking industry. Approximately 25% of all outstanding loans to the private sector were unpaid as of this writing (Oni, 2019). Security concerns are among the most difficult problems the banking industry in Nigeria and throughout the world is now experiencing. Unauthorized access, use, disclosure, interruption, alteration, and destruction of customer information are among the serious dangers to bank customer information that can result in fraud occurrences and negatively impact on the profitability and reputation of several banks in the worldwide marketplace (Islam et al., 2022). As we become more reliant on the Internet, the hazards of online hacking, virus assaults, and other security breaches are rising quickly. Even though banks in developing nations are adding security measures, consumer behaviour is generating security holes. There are still a lot of weaknesses and dangers to Internet security in the world. Although cyber security has grown to be a top issue for the banking sector, several Nigerian banks are hesitant to implement the essential security measures to combat credible threats (Darem et al., 2023). Regulators have also been fast to create measures to handle significant assaults when they happen. Although consumers can obtain their money according to federal legislation, some analysts worry that the growing number of attacks is leading to bank failures and reducing profitability (Darem et al., 2023). As a result, this study looks at how security regulations affect the bottom lines of deposit banks in Lagos State, Nigeria.

A company's total performance can be determined in large part by its profitability (Kanoujiya et al., 2023). According to Kanoujiya et al. (2023), profitability is the capacity of the business to employ its resources to generate revenue greater than its expenses. Put differently, the ability of the business to make money out of its operations. According to Kanoujiya et al. (2023), profit is the ability of a business to use its resources to generate income above its costs. Through business, companies make money. Profitability is contingent upon the company's ability to generate revenue (Creel et al., 2021). A given investment's profitability is determined by how likely it is to yield a profit. Corporate profitability is defined as the company's capacity to create revenue by Abdul Hadi et al., (2018). Profit is the outcome of the combined influence of liquidity, asset management, and management, according to Sulaeman et al. (2019). In a similar vein, profit is the joint product of different management strategies and choice.

As per Srinivas et al. (2019) a security policy often consists of a list of a nation's or organization's top security concerns along with a plan of action to resolve them. To accomplish objectives that support organizational security, security strategies are strategic, all-encompassing, and methodical approaches to resource development, utilization, and coordination (Al-Khater et al. 2020). According to Butun et al. (2019), a good security strategy is broad, strong, and adaptable enough to counteract any kind of security attack. As stated by Srinivas, Das and Kumar (2019), the process of developing a security strategy is extensive and involves several steps, such as preliminary evaluation, planning, execution, and periodic evaluation. The network security, endpoint security, network security, and physical asset security are all part of the comprehensive security plan used in this study.

Effect of Internet Fraud Prevention on the Nigerian Banking Industry

Fraud is a scourge affecting Nigerian banking institutions and the economy. A major impact can be seen in the decline in bank income statements and the recession of the country's economy. Abdallah et al. (2016) concluded that efforts to detect and eliminate fraud in the business sector seem to have little impact because fraudulent activities have recently increased. Nugraha and Bayunitri (2020) describe fraud as "the activities of one or more individuals, managers, employees, or other parties, which may lead to fraudulent financial statements." Fraud, including misrepresentation, forgery or falsification of supporting documents, misuse of assets, concealment or removal of transaction results from records or documents, invalid transaction documents and distorted accounting standards (Singleton & Singleton 2010).

Fraud prevention is the process of identifying suspicious transactions in the banking industry and preventing them from causing financial or reputational damage to customers or other financial institutions (FIs). As online and mobile banking services expand and become more popular, and as financial institutions continue to go digital, having a robust fraud prevention system in place becomes even more important. Cybercrime and fraud prevention are closely related and constantly evolving.

The whole world, and the banking industry in particular, benefits from the speed of power and innovation of information technology, with its multifaceted importance, which continues to facilitate human work in many fields and times i. Digital technology and the Internet of Things are at the heart of this planned transformation. As the Internet is increasingly used for commercial purposes, the number and variety of computer crimes increases. Part of the crime may have been based on electronic devices, but in some cases, many crimes were committed online or through technological processes.

According to Singh et al. (2021) the rise of fraud and crime has forced the development of cyber security. Cyber security aims to reduce, if not eliminate, cyber fraud and other related crimes in the ever-changing human society.

2.2 Emergence of the Internet and Cybercrime

The advent of the internet has changed the way people do things. The Internet has emerged as the world's fastest growing communication tool. In general, its appearance has changed especially in the fields of business, work, consumption, entertainment and politics (Castells, 2020). In 2001, it was estimated that more than 700 million people were using the Internet. In 2007, more than 1 billion people were using electronic mail (email) and more than 240 million people used various mobile devices (Morah & Uzochukwu, 2019). Currently, there are more than 2.8 billion Internet users, of which 641.6 million live in China and 250 million in the United States. These two countries have the most users of any country in the world, but people from almost every country in the world have some kind of online presence. By the end of 2020, there will be six times more Internet devices ("Internet of Things") than humans, completely changing the way we think about the Internet today. In tomorrow's highly connected world, it would be difficult to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked to Internet Protocol (IP) connectivity.

Indeed, the global expansion of computing and Internet devices, such as computers, personal digital assistants (PDAs), and cell phones, is one of the most important technological changes in human history. There is no doubt that the increased capabilities of information technology (IT) are unprecedented and will change the way we work and function as a society (McQuade, 2019). Most people today have multiple services online, with multiple email accounts, both personal and business, and social media profiles on different sites such as Facebook and Instagram. In addition, consumers are increasingly moving away from print media in favour of e-readers and digital book formats (Ketron & Naletelich 2016).

In addition, cell phones, especially text messaging, have become a more popular form of communication than other traditional methods, including face-to-face conversations, letters, phone calls, and even email. In fact, people under the age of 20 are more likely to text than call. Castells (2020) refers to the Internet as a "network of networks." Basically, it is a network that connects computers and allows them to communicate and exchange information (Yar et al., 2021). Most information and communication technology (ICT) networks have been around for decades. Some are used in financial markets, while other large companies such as the military, government agencies, business organizations and universities include them in their activities. In general, the Internet provides a way to connect many different existing networks, and from them to a single network that allows communication between all "nodes" (such as individual computers) create a network (Yar et al., 2021).

The origins of the Internet can be traced back to the development of the network known as ARPANET in the 1960s, taken over by the US military, whose main goal was to establish a way to make communications secure and modern and to coordinate military operations. and the strategic context of the "Cold War," where the threat of nuclear war is always present, such networks ensure that important communications can continue even if a specific "point" within the computer infrastructure is destroyed through an attack seems like a way to ensure it. stability (Yar et al., 2021).

Additionally, ARPANET technology was intended to allow communications to be broken up into "packets" and sent through separate channels to their destinations, where they could be reassembled into their original form. If a middle point in the network fails, it can be routed through another route, ensuring that the message reaches its destination. Creating a network requires not only the right computer equipment, but also the development of a "strategy". Protocols are rules and regulations that allow different computers to "understand" each other. Development began in the late 1960s, and by 1969 the ARPANET was operational, initially connecting a small number of university research communities and government agencies. Beginning in the early 1970s, more innovations such as email appeared, increasing communication opportunities. Other networks like ARPANET have also been built, such as JANET (Joint Communications Network) in the UK and NSFNET (affiliated with the National Science Foundation) in the US. Using common communication protocols, these networks can be connected to form the Internet, a network of networks.

The main force behind the emergence of the Internet came in 1990 when the American authorities put ARPANET under private management under the support of the National Science Foundation ((Yar et al., 2021). Also in 1990, researchers at the CERN physics laboratory in Switzerland developed a browser called the "Wide Web" (www). This application has been improved by other developers to enable more informative ways of sharing information, such as sharing images and text (Yar et al., 2021). The first commercial browser, Netscape, was launched in 1994, and the following year Microsoft launched its Internet Explorer. These browsers make it possible to access the Internet from personal computers (PC). In the mid-1990s, several commercial Internet service providers (ISPs) entered the market, making it possible for anyone with access to a computer and a traditional telephone line to connect to the Internet. Since the Internet was commercialized in the mid-1990s, its growth has been very rapid (Yar et al., 2021).

Today, the word cyber and the related word dot com are probably the most common words in modern times. However, despite the many benefits gained from these technological innovations, people involved in crime continue to use the opportunities of interaction and networks provided by the Internet to commit crimes on the Internet Don't We can use Internet technology to protect against theft, information destruction, copyright infringement , violation of professional secrets, digital privacy, or intellectual property, distribution of illegal content, competitive attacks, industrial espionage, trademark infringement, distribution of false information

and services help many types of crimes such as such as theft, various frauds, and illegal money laundering (Foca 2024). In fact, information technology resources have become increasingly important to cybercriminals. The Internet and the Internet can be considered a criminal environment. The presence of individuals and private or public companies on the Internet contributes to the growth of cybercrime by increasing the number of potential targets for cybercriminals.

Cyberspace, by its very nature, provides an interesting environment for the display of crimes, whether ordinary crimes or crimes that use the possibilities created by information technology (Foca, 2024). In addition, users can control it remotely via the Internet or hide behind the screen. In fact, some people may cross the line and engage in criminal activities without fully realizing the criminal nature of their actions. The computer world offers cybercriminals the possibility to automate their activities. The increasing number of criminal acts carried out remotely over networks, against large numbers of targets, and on a large scale means that criminals can be everywhere in time and space. The removal of transaction materials, communication tools, and encryption and anonymity solutions will allow criminals to connect securely and easily without physical contact. Therefore, criminals can form groups and organize illegal activities carried out through traditional means or ICTs (Foca, 2024).

Computer crime changed into computer-related crime and what is now known as cybercrime with the launch of the World Wide Web in 1993, as well as the introduction of numerous software applications, online content, and high-speed Internet/broadband connections. (Yar et al. 2021). As a result, a conversation about cyberbullying would be lacking if it did not include cyberbullying. Since the former is impossible and non-existent without the latter. According to Yar et al. (2021), the most significant electronic domain where cybercrime takes place is the Internet. It is also incorrect to view the Internet as a standalone technological advancement or as a "blank slate" that exists independently of its users. Rather, one should view the Internet as a set of social norms. Because people use the Internet for different goals and in different ways, it takes on its current form (DiMaggio et al., 2001). To fully appreciate what a fantastic tool the internet is, one must grasp what people do online and how they do it. Criminal and abnormal behaviour is made possible by the social uses of the Internet (Yar et al., 2021).

2.3 Reducing the Economic Costs of Cybercrime

Accurately measuring the economic costs of cybercrime can inform crime reduction efforts, strengthen local, national, regional and international responses, identify gaps in response, and improve understanding and risk assessment and build public education and advocacy (Armin et al., 2016). Therefore, stakeholders at various levels, including government agencies, business groups, law enforcement agencies, and international organizations, are interested in having an accurate understanding of the global economy. The main reason is that knowledge helps in understanding nature, trends and patterns of cybercrime and ultimately helps in designing a strategic plan to deal with the problem. But unfortunately, the economic costs of cybercrime are often very difficult to measure as we do not know the exact statistics of the number of cyber incidents, or the loss of income caused by cybercriminals.

One way to measure new types and dimensions of crime, including cybercrime, is to seek to describe "who" (how many people) and "what" (how many) are involved. This requires a combination of data sources, including information on criminals, including organized crime groups, information on money flows between illicit markets, statistics on crime, damage and loss, and money flows. Each of these factors affects the response to cybercrime. For example, understanding the structure and networks of organized crime groups is fundamental to the design of criminal justice interventions. Additionally, understanding illicit markets, such as the underground economy based on stolen credit card information, can provide basic information on criminal activity (regardless of the individuals or groups involved and thus prevent deterrence). Understanding the extent of harm, loss and illicit profits can guide the prioritization of interventions.

2.4 Performance

Efficiency is the result of operations and is related to the overall efficiency and productivity of any business. Two ways of dealing with work are known in literature. financial or "sales basis" and non-financial or "business basis". Financial is measured in terms of profit, growth, productivity, sales volume, market share, return on investment, value added, while non-financial is measured in terms of employee development, customer satisfaction, etc. degree conditions, job satisfaction, and internal processes of the relevant organization (Thomas et al., 2023). Therefore, strategic management methods are justified based on their ability to improve performance (Emmanuel et al., 2023). According to Omenazu (2022), performance measurement is a way to determine whether the organization is achieving its goals (Makanga, 2021) and it is important to assess the overall health of the organization.

Although a company's performance is considered good when it achieves sales targets or performance-based product targets, performance is considered good when it uses its resources to achieve high levels of activity (Flores-Hernánde et al., 2022). Muchiri and Muathe (2024) refer to an organization's effectiveness in achieving its goals as performance. They also say that performance determines the existence of an organization in the economy, while Suleiman (2024) says that performance determines how the organization uses its resources to ensure that it reaches its set goals. Sources may include the level of transactions between a particular bank and its customers. Other resources are coordinated

by human resources, which are the employees of the organization. Akinlabi et al. (2021) said that the level of performance of the organization depends on the level of productivity and profit, and for the organization to be successful and continue the business, it must have all the necessary equipment to support production and performance, and we should consider to the environment, especially the local area. He added that organizations should also review their external environment and be aware of changes that may affect their work.

Performance is understood as the ability of the company to achieve its goals, that is, to meet expectations, and therefore not only through the results in a broad way, but also through the planning of the goals of the match. However, to measure business performance, you need to track relevant business metrics, also known as key performance indicators, that demonstrate measurable value and signal progress toward business goals. This includes measuring actual business performance against intended goals. It is important to remember that business performance can also be defined as the company's ability to generate maximum business income from the available material and human resources. Njoku et al. (2023) stated that performance is understood as the company's ability to achieve its goals, that is, its ability to meet expectations, and therefore not only through results in a broad sense, but also through a corresponding system of goals. Therefore, performance is primarily determined by a set of multidimensional requirements. The source of performance is the actions of actors in the business process. It is generally known that banking activities involve a high level of risk and a high probability of bankruptcy. Therefore, many agree that banks are one of the most strategic institutions in the world (Chortareas et al., 2024).

Haris et al. (2024) reported a strong relationship between cyber security and profitability. Similarly, Gakure and Ngumi (2018), in their study on the impact of innovation on the profitability of commercial banks, presented results showing that bank savings have a moderate effect on the profitability of banking businesses in Kenya. In a study on the effects of cyber-attacks on financial institutions, Harunurrasyid et al. (2024) found that cyber security affects the profitability of financial institutions and that the impact is significant for direct and indirect losses. A study by Podrecca et al. (2022) founded that the implementation of the ISO 27001 standard for cyber security has a significant impact on the profitability metrics measured by return to equity, and the implementation of the PCI-DSS standard has a significant impact on the profitability metrics their ratio of unpaid debts has been found to affect the quality of Similarly, Abdulazeez and Magaji (2023) shows that cybercrime has a negative impact on income and also affects the profitability of banking companies.

Khalil (2020) investigated the relationship between cyber security costs and financial innovation (product) for banks in Pakistan. Selected banking experts were surveyed as part of this study to collect their responses. According to this study, financial stability of impacted electronic banks is significantly impacted by investments made in cyber security. Thus, to enhance the bank's overall performance, we advise banks to consistently step up their efforts to develop novel products.

Njoroge (2020) evaluates the connection between financial innovation and cyber security. To collect data, a controlled questionnaire was employed in conjunction with a descriptive study methodology. In this study, financial innovation in Kenyan banks is positively correlated with cyber security costs as determined by preventive and detection costs; however, this relationship is not statistically significant. However, there is a positive and statistically significant impact on financial innovation from other direct expenditures like legal fees and business continuity costs. The research findings urge banks to keep up their efforts to develop more cutting-edge banking services and products.

Wang et al. (2020) assessed cyber security breaches, practices, and capacities to assess internet banking in Nigeria. This study employed a descriptive research approach, and a sample of one hundred seasoned banking professionals participated in an online survey. The results show that cybercrime's severity and present level of vulnerability in Nigeria's banking industry are rising quickly. The report suggests enforcing stricter laws and implementing new, more potent Internet technology tools to halt this trend.

Ogunwale (2020) examined the effect of cyber security on the operations of Nigerian savings institutions using a theoretical framework. Multiple regression analysis was carried out on the gathered monitoring data. According to our findings, banks' financial performance is positively impacted by adequate cyber security measures. According to the study's findings, enforcing all applicable cyber security legislation will contribute to a decrease in cybercrime and foster public trust in the banking sector.

Measures to lower the frequency of fraud in Nigeria's banking sector were examined by Idowu et al. (2022). Poor working conditions, ineffective administration of regulations and procedures, and disgruntled staff who endure long hours owing to low compensation are just a few of the variables that the study found contribute to the prevalence of fraud in banks. The usefulness of novel knowledge dissemination characteristics was examined in a follow-up study by Nyirambyeyi (2018). In this research, the target innovation in the financial sector is automated teller machines (ATMs). This investigation showed that attitudes play a major role in how often ATMs are used in banks, which in turn influences the performance of the bank.

According to research by Nwarize (2023), bank clients trust and rely on the usage of specialized equipment in banking operations, particularly ATMs, which allow them to conveniently meet their financial demands. In Japan, ATM fraud is increasing. As ATM fraud occurs frequently and cybercrime techniques become more sophisticated, institutions must manage the risks involved and mitigate their impact. "Challenges related to the use of Automated Teller Machines (ATM) and the

incidence of bank fraud in the Nigerian banking system" was the subject of John and Rotimi (2014) investigation. The study found that the primary causes of bank fraud include inadequate leadership abilities, communication breakdowns, and a lack of appropriate training. It suggests setting up suitable internal control protocols and giving suitable guidance for worker comfort, pleasure, and other advantages.

Onapajo and Uzodike (2014) investigated fraud and judicial analysis in Nigeria in a different study conducted there. The study showed that Nigerian banks needed to be more proactive in the system, implementing good accounting practices, for example. Idolor (2010) study looked at how fraud affected Nigerian banks' operations. The findings indicate that the overall amount of money involved in fraud and bank profitability are significantly correlated. Chukwuekwu (2024) also used descriptive statistics to examine the nature, extent and economic impact of bank deposit fraud in Nigeria. This study examines the positive relationship between bank deposits and fraud in the Nigerian banking sector.

Abrifor et al. (2024) investigated how bank fraud affected Nigeria's economic growth. The study spans the years 1995 through 2014. Secondary data is used in this study's analysis. Data analysis was done using SPSS application software and regression analysis. The results of the study showed that bank fraud hinders Nigeria's economy's growth. Any society's potential for economic growth and development is contingent upon the degree to which financial services are rendered with assurance, trust, and low risk. Naturally, these call for safe and sound banking practices, which most Nigerian banks now disregarded at their own risk. According to the report, Nigerian banks should hire with caution and enhance their management. Large returns alone are insufficient; you also need to take your employees' honesty and their fear of God into account. The study concluded that measures must be taken to identify, deter, and retaliate against fraudsters to lessen the temptation to conduct fraud and enhance the possibility of detection. While the latter can be accomplished with an efficient internal control system, the former demands constructive changes to the work environment.

Chukwuekwu (2024) in his research on banking crime, noted that society’s perception of financial resources, position in the social situation, economic development, people's expectations of bank employees, and its consequences. He points. It turns out that social and economic deficits in the economy, as well as the need to meet expectations, contribute to cyber violence. The role of bank managers in significant corporate fraud in the Nigerian banking industry was examined by Otusanya (2020) in a different study. Studies reveal that bank executives in Nigeria's recent banking crisis have been involved in corruption and fraud. These executives have been trained in the American Dream Theory; a theory that suggests love increases the likelihood of financial crime.

Ibekwe (2021) investigated the relationship between financial innovation and financial performance of deposit banks in Nigeria. Data for this study were collected from Central Bank of Nigeria Statistical Bulletin, CBN Annual Report, and Accounts Bulletin, and analysis was done using multiple regression tools. This study produced mixed results regarding the different agents used. ATM, POS, and mobile banking (as a proxy for financial innovation) have a statistically significant positive effect on game performance, while internet banking (as a proxy for financial innovation) has a statistically negative effect on violence of game performance.

Osi et al. (2024) analysed the relationship between cyber security and audit committee effectiveness in relation to listed deposit banks operating in Nigeria. This study uses the methods of exploratory research design and makes non-significant calculations with the help of regression and correlation analysis tools. The findings of this study show that the current characteristics of audit committees in Nigeria cannot positively influence cyber security measures. Therefore, the researchers recommend urgently improve the structure of audit committees by hiring more technical staff.

Leukfeldt and Holt (2022) researched the issue of cybercrime using a sample of 37 criminal networks. Their results show that different cybercriminals engage in different types of crime. They may be involved in specific types of crime, with about half of the criminals in this sample turning out to be cybercriminals, and the other half committing a variety of online and offline crimes. The relative balance of intelligence and innovation, especially in online and offline activities, suggests that the designation of fraudsters as a distinct criminal group may not be worth much. From their research, they raise the question of what influences the entry of criminals into cybercrime, whether they are sophisticated criminals or general criminals. Large cybercriminal networks may have helped cybercriminals, whether professionals or public officials, to identify and exploit opportunities to commit fraud, extortion and other financial crimes.

Herrero et al. (2021) study combined data on Internet addiction, activities of daily living (L-RAT), and self-control theory (SCT) to model smartphone users' vulnerability to the internet. This method, which is known as duality in relation to the development of cyber security, is being tested without exception on a sample of mobile devices across the country. Data from 2,837 Spanish power users from a national survey were sampled using the Mplus sampling software. The results of the study show that L-RAT and SCT predict cybercrime victimization (high sensitivity, closeness, appropriateness, absence of cognitive moderators, and low self-control). In addition to the predictor effects of L-RAT and SCT, it is also proven that mobile phone dependence significantly affects the probability of hacking. Potential victims of cybercrime exhibit two types of vulnerability. The first is the risk identified in crime theories such as L-RAT and SCT, and the second is due to the misuse and implementation of web access devices (mobile phones in our study).

Reveron (2012) cyber environment to improve national security and promote the digital economy. In addition,

Ratzinger-Sakel and Tiedemann (2022) used primary sources covering the 10-year period from 2010 to 2020 and found that although foreign accounts do not completely control the detection of fraud, investigative accounting has a positive and significant effect on fraud prevention I found to provide. We also find that a court case has no apparent beneficial effect on the recovery of fraudulently stolen funds.

Otusanya and Adeyeye (2022) research shows that Nigerian commercial banks are facing threats and failures that can lead to the destruction of billions of dollars in assets, money laundering and the collapse of the country's critical infrastructure. Researchers propose to develop a cybercrime classification system that can identify cybercrime more accurately compared to current methods.

Efiong et al. (2016) conducted a data analysis using a survey method to examine the effectiveness of prevention and detection strategies. The study identified several strategies to reduce crime in Nigeria, including a strong internal control system.

Akinleye Gideon and Akadi Omolara (2024) investigated the impact of professional audit on money laundering in Nigeria (DMB). Voting is done by crossvoting. Participants in the study were employees of the banking and auditing sector in Abeokuta in Ogun state. The results show that forensic audit has had a significant impact in the fight against financial fraud in Nigeria (DMB). The P-value of the expert audit report significantly improves the court judgment on financial fraud in Nigeria, with a P-value of less than 0.05, and the expert audit report significantly improves the court judgment on financial fraud in Nigeria. Research shows that the use of judicial review to combat money laundering in Nigeria (DMB) is still in its infancy. In a similar study titled "Effect of Scientific Research Methodology on Business Fraud Prevention in Nigerian Banks".

Baba (2019) and Alao (2012) investigated the effectiveness of forensic methods in preventing corporate fraud in Nigerian banks. This study uses an exploratory research method, using data from primary sources such as conducting interviews and questionnaires, and secondary sources such as financial fraud and counterfeiting complaints. This study shows a strong relationship between forensic methods and corporate fraud prevention. Statistics show that although fraud cases often require the skills of a forensic investigator, they often do not.

Alao (2012) investigated the impact of fraud on bank failure in Nigeria. This study adopted a cross-sectional survey and a post-survey method. The results of the study show that the incidence of fraud does not have a significant effect on the total loss of Nigerian banks, with a P value of 0.972 greater than 0.05, and that the incidence of fraud does not have a significant effect on the expected total loss of Nigerian banks I find it inappropriate. According to this study, the amount involved in bank fraud in Nigeria is a reliable indicator of bank failure.

Nugraha and Bayunitri (2020) investigated the effect of internal control in preventing fraud in BRI Bank in Cimahi City. The research method used in this study is a descriptive method. The sample size of this research is 46 employees of Bank BRI in Cimahi city. The analytical method used in this study is a one-sided hypothesis test (T-test) with a significant level of 5%. The software used for data analysis was the Statistical Package for Social Sciences (SPSS) version 20.00. According to this study, internal control has a significant effect of 50.2% in preventing fraud.

Awale and Kulmie (2024) research sample was randomly selected, and the total respondents were 171 external auditors working in CPA firms in Indonesia. The results show that moral development and education have a significant effect on detecting fraud, but CPE fraud has no effect on detecting fraud.

Anumba (2023) investigated several challenges in detecting and preventing fraud in the Nigerian banking sector. According to the results of the descriptive research, the main type of fraud in Nigeria is money laundering by bank directors and managers instead due to lack of motivation. In addition, governments are encouraged to support anti-corruption agencies and improve their financial independence. Managers and directors involved in embezzlement should be prosecuted to prevent future fraud. Before hiring a bank, you should do proper research and assess their ethics and integrity.

Renugadevi et al. (2024) developed IoT monitoring to remotely monitor the output of the PV system and enable ensuring the distribution of ventilators and monitors in the ICU room at RSI Siti Khadijah Palembang that I researched. The method implemented in this study is to install IoT monitoring as an automatic transfer switch to ensure continuous distribution to the load. IoT monitoring shows real-time output of PV panels, battery capacity, and inverter output. Therefore, operators can monitor the results of the PV system and decide whether to continue using power from the PV panels or switch to the grid on cloudy or rainy days. This study shows the effectiveness of implementing IoT monitoring on a grid PV system installed at RSI Siti Khadijah Palembang.

The Center for Computer Security conducted a survey of government agencies asking if they had experienced a cyber-attack (Rudasill & Moyer, 2004). The purpose of this study is to have a more accurate picture of the number of crimes on the Internet. The institute surveyed 5,412 security professionals through traditional mail and email, asking them about cybercrime that occurred between July 2009 and July 2010. A total of 351 surveys were completed and returned. Of the 351 respondents, almost half (49.8%) did not have a security incident in the past year, 41.1% experienced a similar cyber security incident, and 9.1% were not sure. Of those who were attacked, 21.6% said they were victims of a targeted attack, 54.5% said it was not targeted, and 24% said they could not determine the type of attack. 5 This shows that although less than half of the security personnel have admitted to being attacked, a large number (about 9%) do not know if they have been attacked. According to the

survey results, the most common type of attack is malware, reported by 67.1% of participants who have experienced an attack. Only 8.7% of these respondents reported incidents of financial fraud. Some respondents were willing to share information about the financial loss their companies suffered because of the attacks, but they said the loss was not due to domestic crime. In fact, 59.1% believed that there was no loss due to the bad behaviour of the auditor, but only 39.5% said that none of their losses resulted from the bad behaviour of the auditor (Rudasill & Moyer, 2004).

The Norton Cybercrime 2021 report is based on an annual survey of government officials in 24 countries about their experiences with cybercrime. The survey included Australia, Brazil, Canada, China, Colombia, Denmark, France, Germany, India, Italy, Japan, Mexico, the Netherlands, New Zealand, Poland, Russia, Saudi Arabia, Singapore, South Africa, Sweden, Turkey, and the United of the United Arab Emirates, United Kingdom, and American officials (Hill & Marion, 2019). The agency conducted an online survey of 13,018 adults between the ages of 18 and 64. The results of the 2012 report found that 556 million people are victims of cybercrime each year, or 18 victims every minute. It is estimated that there are 1.4 million people who abuse the Internet every day. Additionally, research shows that consumer cybercrime costs approximately $100 billion annually.

Anderson et al. (2013) also conducted an annual survey on cybercrime, and the report found that the number of cybercrime attacks and the costs associated with them have increased for the third year in a row. The study looked at cybercrime in the US, UK, Japan, Germany and Australia. The results show that the number of attacks has more than doubled since 2010, and the economic cost to businesses has increased by almost 40%. However, the rate of increase seems to be slowing down. In total, there are an average of 102 successful cyber-attacks every week. More than a quarter of these attacks are due to malware, denial of service, stolen or stolen devices and malware (Anderson et al., 2013).

3. METHODOLOGY

An exploratory strategy was employed in this study to create a framework for analysing the features of the independent variables. This is helpful in describing the current condition of the research variables and obtaining information about the event's status. The research approach in this study made it very easy to obtain precise information from the respondents. The workers and clients of the five UBAs in the Federal Capital Territory (FCT) of Abuja stand to gain from this study. Each bank's workers and customers provided 121 replies to the poll. Naturally, the process of carrying out this study necessitates an awareness of consumers for researchers to contribute and share their experiences, which will result in successful cyber security initiatives (Table 1).

Table 1. Distribution of total population

The bank's response	Total population
UBA, Ouse	thirty thousand
UBA, Infection	twenty-four
UBA, central region	thirty thousand
Mom, Javi	three and twenty
FATHER, Gwarinpa	twenty-four
together	121

Source: *survey data, 2023.*

Table 1 shows the total distribution of workers where we examined a total of 121 people. A total of 26 respondents were collected from the Wuse department, 24 from UBA Asokoro, 25 from UBA Central area, 23 from UBA Jabbi and 24 from UBA Gwarimpa located in the central business district of Abuja. Depending on the kind of target population, the sample size may be large or small. There are 121 studies in total. The sample size is established at 121 individuals. A 95% confidence level and a 5% margin of error were used to calculate the sample size. This study's sampling strategy is a straightforward random sampling strategy. To ensure that every person of the population has an equal chance of being selected, a straightforward random sampling procedure is used. Because surveying a sample is less expensive than surveying the complete population, simple random sampling is utilized. Comparing studies of the entire population to this one also enables more thorough research and quicker results.

Primary sources provided the data for this research. Using questionnaires and interviews—two methods used in the research process—we gather data. Questionnaires, which were created based on the factors determined to be crucial for achieving the study's goals, were the instrument used to gather research data. A questionnaire with both open-ended and closed-ended questions will be given to respondents. The usage of questionnaires stems from their ease of administration and the ease of analysis of the data they gather.

To acquire data for this study, oral interviews and questionnaires are used as primary sources. The research's structure, design, and methodology are intended to address the research questions and guarantee the accuracy of the pertinent data gathered. There are two sections to the study. In Chapter 1, respondents' demographic information is the main topic, and in Chapter 2, questions concerning the effect of cyber security on the operations of commercial banks in Abuja, Nigeria, are the focus.

4. DISCUSSION AND ANALYSIS

Frequency was used in this study to represent the number of times each symbol appears. To enable researchers to compare replies accurately, frequencies were transformed to percentages (%). By converting the frequency reading to a percentage and utilizing the

conventional "100" standard as a reference, the number per 100 is displayed.

The analysis was conducted using SPSS 20.0, a statistical software program. ANOVA and linear regression models are two statistical techniques that are applied, depending on the issue or query. After collecting the data, the data will be coded, presented, and further analysed. The researcher first produces a table that is given as output from the computer. Descriptive, frequency and correlation analyses were obtained to describe the characteristics of the subjects in the organization. Pearson's correlation coefficient was used to determine how the research variables related, and regression analysis was used to determine the impact of cyber security on the performance of United Bank for Africa, Abuja (dependent variable, cloud security implementation, internal effectiveness. control, and commitment of the organization) and the independent variable, that is, employee productivity.

UBA, Abuja reported that 91 (75.2%) respondents strongly agreed, 6 (4.9%) agreed, 8 (6.6%) were unsure or undecided, 9 (7.4%) disagreed, and 7 (5.7%) strongly disagreed that implementing cloud security has a major influence on productivity. According to Abuja officials, the aggregate response to this issue was 3.66 on a Likert scale, indicating that respondents agreed that United Bank for Africa's productivity will grow with the introduction of cloud security.

Regarding "Cloud security protects customer orders, templates, and financial information," 89 respondents (73.5%) highly agree, 15 agree (12.3%), and 8 are doubtful. Of those who are undecided, 6 disagree (4.9%), and 3 strongly disagree (2.4%). On a Likert scale, the mean response for this question was 3.70, meaning that respondents generally agreed that internet security safeguards templates, orders, and consumer financial information.

Point 3, "Customers are confident that their accounts are safe with the implementation of cloud security," Six respondents (4.9%) and 90 (75.2%) strongly agreed with the statement. Not sure/undecided, disagree, 7 (5.7%) disagree, and disagree, 9 (7.4%). According to the Likert scale, the overall response for this question is 3.88, meaning that the respondents agree. Your customers will feel secure knowing that their accounts are secure with you thanks to cloud security. The average score for all items is 3.89 indicating agreement on the Likert scale, indicating that the respondents agree with the above statement regarding the implementation of cloud security and productivity in United Bank for Africa, Abuja.

Article 4 of the research, "The implementation of good internal control has a significant impact on the performance of the African Union Bank, Abuja," Eight respondents (6.6%) and 83 respondents (68.5%) agree. Ten (8.2%) people agree, eleven (9.0%) disagree, and nine (7.4%) disagree. The Abuja production revealed that the respondents agreed that there is a strong association between good internal control and the United Bank for Africa, as indicated by the overall response of 4.09 on the Likert scale.

Table 2 Research Question: How does material security affect productivity in UBA, Abuja?

Recently	**research questions**	**something**	**SA (%)**	**(%)**	**UD (%)**	**(%)**	**SD (%)**	**(%)**	**foreign currency**	**total**
7	RQ3: Effective material security Operation	Material security affects productivity at the African Union Bank in Abuja.	81 (66.9%)	16 (13.2%)	8 (6.6%)	9 (7.4%)	7(5.7%)	121 (100%)	531	3.85
8		Effective material security has a significant impact on productivity at the African Union Bank in Abuja.	79 (65.3%)	20 (16.5%)	9 (7.4%)	7(5.7%)	6 (4.9%)	121 (100%)	698	4.08
9		Application security protects your bank's image	90 (75.2%)	6 (4.9%)	9 (7.4%)	9 (7.4%)	7(5.7%)	121 (100%)	647	4.00
					joint part		3.93			

Source: *researcher estimate, 2023*

The survey indicates that 89 participants (73.5%) strongly agree, 15 (12.3%) agree, and 8 (6.6%) agree with item 5, "Interactive implementation helps protect customer accounts." Three (2.4%) people strongly disagreed, while the remaining 4.9% were indifferent. Respondents generally agree that putting controls in place helps protect client accounts, as indicated by the Likert scale response of 3.87 for this item. Research question 6: "When internal control is applied successfully, customers can be sure that with 3.91, 75

(61.9%) respondents strongly believe, 9 (7.4%) disagree, and 7 (5.7%) are not sure/undecided. Respondents agree that working alongside coworkers from varied backgrounds influences their decision-making, as indicated by the overall response of 3.91 on the Likert scale. On the Likert scale, the absolute mean of all questions is 3.95, which indicates agreement. This means that the respondents concur with the comments stated regarding increased productivity and internal control.

81 (66.9%) of the respondents agreed with Article 7's findings that "Good material security has a positive effect on productivity in the African Union Bank, Abuja," whereas 16 (13.2%) and 8 (6.6%) disagreed. Nine (7.4%) disagree, seven (5.7%) strongly disagree, and seven (not sure/undecided). Effective material security at the United Bank for Africa, Abuja, has a favourable impact on productivity, according to participants, who agreed overall with a Likert scale score of 3.85 points. What it does is demonstrated in item 8: "Good material security has a significant impact on productivity in the African Union Bank, Abuja" revealed that 20 (16.5%) respondents agreed, 79 (65.3%) agreed, 9 (7.4%) are unsure or undecided, 7 (5.7%) disagree, and 6 (4.9%) strongly disagreed (Table 2).

At UBA, Abuja, the average response to this item is 4.08, indicating agreement on the Likert scale, suggesting that material security has a major influence on productivity. Regarding the statement, "Proper application security protects the bank's image," participants highly agree, 6 (4.9%) agree, 9 (7.4%) are unsure or undecided, 9 (7.4%) disagree, and 7 (5.7%) disagree. Better material security is indicated by the overall score of 4.00 on the Likert scale, which indicates agreement. According to the Likert scale, the partial mean for all questions was 3.93, which indicates agreement. This means that the respondents agreed with the prior statement regarding adequate equipment protection as well as labour.

Table 3. Analysis of the relationship of research parameters

		CSI	**Editor-in-Chief**	**EA**	**Associate Professor**	**FI**	
CSI	r	1					
Editor-in-Chief	r	-0.036	1				
EA	r	-0.004	0.047	1			
Associate Professor	r	-.098 *	.281 **	-.076 *	1		
FI	r	0.038	.232 **	-.105 **	.274 **	1	
	never	121	121	121	121	121	
* Correspondence is significant at the 0.05 level (two-tailed).							
** Correspondence is significant at the 0.01 level (two tailed).							
Key: A dynamic definition							
CSI	Implementing cloud security						
Editor-in-Chief	effective internal control						
EA	Effective application security						
Associate Professor	Operation						
FI	financial innovation						

Source: *Compiled by researchers, 2023*

The correlation coefficients between cyber security and performance, as determined by this study, are displayed in Table 3 above. Strong correlation between variables is shown by correlation values ranging from -1 to +1 and 0.75 to 0.99. Strong correlation between intercept variables is implied by correlation values 0.5 to 0.74 and 0.35-0.49, respectively (Table 3).

4.1 Hypothesis Testing

Three null hypotheses were tested using regression model analysis techniques to address the study questions and meet the objectives. Table 4 illustrates the relationship between improved software security and reliable change production, whereas regression model illustrates the impact of cloud security implementation and robust local controls on reliable production.

Table 4. Summary of the model

example	**R**	**R squared**	**The right square of R**	**standard error of estimate**
1.	.398a	.158	.155	1.06145

a. Forecast: (regular), implementation of cloud security, better internal control

Table 4 above demonstrates that the square root R of 15.8% indicates the combined information power of the performance (staff productivity) and cyber security parameters (implementation of cloud security and effective internal control). Our approach excludes about 84% of the influence of other unrelated factors.

Table 5 Regression analysis of variance
Analysis of variance

example	total plots	df	mean square	debt	Correct
reaction	144.157	3	48,052	42,650	00 billion
The rest	766.140	680	1.127		
together	910.297	683			

a. Dependent variable: employee performance
b. Forecast: (Continuous) implementation of cloud security and better internal controls

Also, from Table 5 of the ANOVA regression model, it is observed that the p-value of the F-test is 0.000, which is a significance level of less than 0.05 (5%), therefore, all variables of cyber security in general they can easily. be easy. found to have a significant impact on production.

Table 6. Regression model coefficient [a]
assignment [a]

example	not measured assignment B	common mistake	standard assignment	t	Sig
to continue	1.476	.167		8.828	.000
Implementing cloud security	.044	.033	.048	1.329	.184
effective internal control	.176	.036	.179	4.822	.000

a. Dependent variable: employee performance
Note: The parameters of the regression models on Table 6 were used to interpret research hypotheses 1, 2.

H $_{01}$: The implementation of cloud security does not have a significant effect on the productivity of UBA, Abuja
To activate the initial null hypothesis, H_{01}, utilize the first parameter. At the African Union Bank in Abuja, implementing cloud security has no discernible effect on output. 0.044 is the regression coefficient for the cloud protection variable (table 6). This indicates that the African Union Bank in Abuja is experiencing an increase in productivity due to cloud security. Thus, as assessed by management, enhancing the cloud security of the banking system may raise United Bank for Africa, Abuja's productivity by 0.044 degrees. Furthermore, the coefficient is not statistically significant because the cloud security p-value of 0.184 is higher than the significance level of 0.05 (5%). In light of this, the null hypothesis—which states that "the implementation of cloud security has no significant impact on the productivity of United Bank for Africa, Abuja"—is rejected. Thus, even if a positive relationship is seen, we infer that the relationship between cloud security and employee productivity is general.
These findings are in line with other researches, which examined the effect of cyber security on the operations of Nigerian savings banks using a theoretical framework. Multiple regression analysis was carried out on the gathered monitoring data. The study's findings demonstrate that strong cyber security practices improve banks' financial performance. According to the study's findings, enforcing all applicable cyber security legislation will contribute to a decrease in cybercrime and foster public trust in the banking sector.
The research findings indicate a noteworthy and affirmative association between cyber security and the operational efficiency of commercial banks.

H_{02} : The implementation of effective internal control does not have a significant effect on the productivity of UBA, Abuja .
It is employed to enable 02. The African Union Bank, Abuja's productivity is not greatly impacted by the adoption of efficient internal control. For the "effective internal control" parameter, the regression coefficient is 0.176. This indicates that the African Union Bank in Abuja's productivity is positively impacted by efficient internal control. According to the respondents, United Bank for Africa, Abuja's productivity may rise by 0.176 points if internal control measures are implemented more successfully. Additionally, the positive internal control's p value of 0.000 indicates that the coefficient is statistically significant because it is less than the significance level of 0.05 (5%). As a result, the null hypothesis—that "the African Union Bank, Abuja's productivity is not significantly affected by the implementation of good internal control"—is rejected. Thus, it can be said that there is a broad and positive correlation between effective internal control and worker productivity.
In their study, Ambe and Ebi (2022) research shows that commercial banks in Nigeria are facing threats and scams that can cause damage of millions of dollars, theft of money and destruction of important national resources. The researchers propose to develop a cybercrime classification system that can detect cybercrime more effectively compared to current methods.

Table 7. Summary of the model

example	R	R squared	The right square of R	standard error of estimate
1	.437a	.191	.188	1.17099

a. Prediction: (frequently), better defensive equipment

Table 7 above illustrates how the combined power of information of the network security parameters (excellent material security) is represented by the square root R of 19.1%. Our model does not account for about 81% of the effects of other unimportant variables.

Table 8. Regression analysis of variance

example	total plots	df	mean square	debt	Correct.
reaction	220,458	3	73,486	53.591	00 billion
The rest	932.435	680	1.371		
together	1152.893	683			

a. Dependent variable: employee performance
b. Prediction: (Frequently) Better material protection

Furthermore, it is verified with all network security characteristics taken together that the p-value of the F test is 0.000 and the level of significance is not less than 0.05 (5%), according to Table 8 of the ANOVA regression model (Table 8). That is crucial influence on employment in Africa.

Table 9. Regression model coefficient [a]

example	not measured Amendment B	common mistake	standard beta coefficient	t	Correct.
to continue	1.367	.184		7.413	.000
Effective application security	.077	.037	.074	2.091	.037

a. Dependent variable: employee performance

The regression model coefficient table 9 above is used to interpret research hypothesis 3.

H 03 : Effective material security has no significant effect on the productivity of UBA, Abuja .

The African Union Bank in Abuja uses it to enable 03—The security of operational equipment has little effect on production. 0.077 is the Material Security Effectiveness variable's regression coefficient. Thus, increased material security at the African Union Bank in Abuja has a beneficial impact on production. Thus, it is hypothesized that enhancing the effectiveness of the commercial bank's equipment security can result in a 0.077-degree improvement in United Bank for Africa, Abuja's employee productivity. Additionally, the best material security's p-value is 0.037, below the 0.05 (5%) significance limit, indicating that the coefficient is statistically significant. This means that the null hypothesis—which states that "Good material security has no significant effect on the productivity of the African Union Bank, Abuja"—is disproved. As a result, it may be said that the United Bank for Africa in Abuja found a general correlation between material security and productivity.

Additionally, Anderson et al. (2013) carried out an annual assessment on cybercrime, which revealed that for the third year in a row, both the quantity of cybercrime attacks and the expenses related to them have increased. Cybercrime in the US, UK, Japan, Germany, and Australia was examined in the study. According to the findings, there have been over twice as many attacks since 2010, and firms are now spending over 40% more. Still, there appears to be a slowdown in the rate of increase. Every week, there are 102 cyberattacks that are successful. Malware, denial of service, stolen or stolen devices, and malware are the causes of more than 25% of these attacks (Anderson et al., 2013). Ahmed et al. The personnel of banks should be trained to spot indicators of online fraud, such as emails requesting website visits or pop-up advertisements promising free merchandise in exchange for passing a physical examination. Lastly, financial institutions must push staff members to inquire about any files, links, and webpages they come across online.

After conducting our own independent investigation, we found a strong correlation between performance and improved hardware security.

5. CONCLUSION

This study looks at how several Nigerian banks perform in relation to internet fraud. The study's data came from primary and secondary sources, mostly respondent questionnaires and the Commercial Bank of Nigeria's statistics journals. Commercial banks are the dependent variable in this study, whereas the independent variables are the historical value of commercial banks, the value of reported fraud cases, the amount lost because of fraud, and the number of employees participating in fraud. We discovered that there is a negative correlation between bank performance in Nigeria and the quantity of money involved in fraud, the amount lost because of fraud, and the number of workers implicated in fraud. However, there is a strong correlation between bank deposits in Nigeria and the immediate value of those deposits.

For our nation to exist, cybercrime must be eradicated or reduced to a minimum. The study focuses on the many forms of cyber fraud, its causes and effects, as well as the difficulties and remedies for stopping it in Nigerian banks. In Abuja, Nigeria, at the African Union Bank, the study was carried out. Even if we have offered several solutions to stop this crime from occurring in the future, commercial banks and their clients can still take many steps to lessen it. Strengthening information technology, especially cyber security, is necessary to lower the amount of fraud and related crimes, which still exist in Nigeria and take many different forms. These findings lead to the conclusion that cloud security increases the statistical likelihood of preventing fraud in the African Union Bank.

6. RECOMMENDATIONS

The following recommendations are made. The report suggests, among other things, that bank management improve internal control procedures and thoroughly screen candidates before employment. This is because staff in banks initiate most fraud prosecutions.

Another effective method of preventing fraud is to keep track of significant transactions using corporate banking regulations and bank identity numbers. In the Nigerian financial industry, the policy of preference and "talking" systems is still in place. They can therefore be vigilant by depending more on fraud detection techniques.

Preventing fraud in commercial banks is critical to instilling confidence in bank customers that their money is secure and to entice both domestic and foreign investors to make attractive, safe investments in the banking sector. However, failing to do so may expose

them to penalties and charges for fraud in commercial banks.

To help strengthen the state of the Nigerian banking system, it is advised that the government create additional anti-fraud and anti-corruption organizations considering the results.

Considering the results, the Nigerian banking industry must improve its internal control framework to thwart fraud and safeguard assets. To monitor and avoid cases of fraud in the Nigerian banking system, banking regulations and regulatory bodies need also tighten their oversight. To do this, they should use all available means.

References:

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, *68*, 90-113.

Abdul Hadi, A. R., Hussain, H. I., Suryanto, T., & Yap, T. H. (2018). Bank's performance and its determinants: evidence from Middle East, Indian sub-continent and African banks. *Polish Journal of Management Studies*, *17*(1), 17-26.

Abdulazeez, H., & Magaji, S. (2023). Nexus between Banking Cybersecurity Breaches, Cyber Vulnerabilities, and Kidnap for Ransom in Nigeria: A Comparative Analysis of Kaduna and Abuja Metropolis, Nigeria. In *Cybersecurity for Decision Makers* (pp. 279-292). CRC Press.

Abrifor, C. A., Egbo, A. K., Ojo, O. T., Ojiziele, M. O., Akan, K. A., Atinuke, T. B., ... & Adebayo, A. A. (2024). Collaborative Bank E-Fraud and Customers' Reactions in Ado-Ekiti Metropolis, Ekiti State, Nigeria. *African Journal of Business and Economic Research*, *19*(3), 483.

Adebiyi, S. O., & Olayemi, G. A. (2022). Predicting the Consequences of Perceived Data Privacy Risks on Consumer Behaviour: An Entropy-TOPSIS Approach. *Studia Humana*, *11*(2).

Akinlabi, B. H., Olalekan, A., & Olaide, M. (2021). The Effect of External Business Environment on Performance of Smes in Nigeria. *International Journal of Advances in Engineering and Management*, *3*(1), 762-774.

Akinleye Gideon, T., & Akadi Omolara, V. (2024). Forensic accounting and corporate fraud in deposit money banks in Nigeria. *Journal of Financial Analysis and Investigation*, *23*(1), 98-115.

Akintoye, R., Ogunode, O., Ajayi, M., & Joshua, A. A. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. *Universal Journal of Accounting and Finance*, *10*(3), 643-652.

Alao, R. K. R. (2012). *Use of direct mail for improved electoral education that encourages civic behavior and election credibility*. University of Phoenix.

Alketbi, A. H. S. B., Jimber del Rio, J. A., & Ibáñez Fernández, A. (2022). Exploring the role of human resource development functions on crisis management: the case of Dubai-UAE during Covid-19 crisis. *Plos one*, *17*(3), e0263034.

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE access*, *8*, 137293-137311.

Ambe, K. N., & Ebi, N. J. (2022). Contemporary Crimes Prevalent within Africa's Banking Industry and a Threat Analysis of Such Crimes on Africa's Development. *Available at SSRN 4217275*.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. *The economics of information security and privacy*, 265-300.

Anumba, M. O. (2023). *Strategies for Reducing Operational Bank Fraud in Nigeria* (Doctoral dissertation, Walden University).

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in human behavior*, *38*, 304-312.

Armin, J., Thompson, B., & Kijewski, P. (2016). Cybercrime economic costs: No measure no solution. *Combatting cybercrime and cyberterrorism: Challenges, trends and priorities*, 135-155.

Awale, A. A., & Kulmie, D. A. (2024). Public employees' views on corruption and financial crimes: A perceptual study. *Journal of Asian Scientific Research*, *14*(4), 612.

Baba, L. L. (2019). *Effectiveness of forensic accounting services in financial crime detection and prevention in selected Public organizations in Dar Es Salaam Tanzania* (Doctoral dissertation, Kampala International University, College of Economics & management.).

Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), 616-644.

Castells, M. (2020). The information city, the new economy, and the network society. In *The information society reader* (pp. 150-164). Routledge.

Chortareas, G., Kostika, E., & Pelagidis, T. (2024). The central bank digital currency dimension in global financial integration. In *Handbook of Financial Integration* (pp. 606-642). Edward Elgar Publishing.

Chukwuekwu, O. (2024). Fraud and performance of listed deposit money banks in Nigeria: Exploring the combined effects of fraud triangle and fraud diamond theories. *Journal of Business and Econometrics Studies*, *1*(3), 1-8.

Congdon, T. (2022). Can the Eurozone Manage Its Free Rider Problem?. *Inflation Rising*, 2022(2), 61-71.

Creel, J., Hubert, P., & Labondance, F. (2021). The intertwining of credit and banking fragility. *International Journal of Finance & Economics*, *26*(1), 459-475.

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, *11*, 125138-125158.

DiMaggio, P., Hargittai, E., Neuman, W. R., & Robinson, J. P. (2001). Social implications of the Internet. *Annual review of sociology*, *27*(1), 307-336.

Efiong, E. J., Inyang, I. O., & Joshua, U. (2016). Effectiveness of the Mechanisms of Fraud Prevention and Detection in Nigeria. Advances in Social Sciences Research Journal, 3 (3), 206-217. DOI: 10.14738/assrj.33.1894

Emmanuel, I. E., Esther, L. O. O., Attayi, I. F., & Taiwo, O. S. (2023). Strategic Management and Performance of Information Technology Firms in Nigeria. *Advancement in Management and Technology (AMT)*, *3*(3), 38-49.

Flores-Hernández, E. R., Rodero-Cosano, M. L., & Perla-Cartagena, A. E. (2022). *Complexity of Family Businesses in El Salvador: A Structural Equation Model. Sustainability 2022, 14, 6773*.

Foca, A. C. (2024). The impact of the Ukrainian-Russian war on European cybersecurity. *EURINT*, *11*(1), 259-272.

Gakure, J. & Ngumi, T. (2018). Bank Innovations Influence Capital Turnover of Commercial Banks in Kenya, Interfaces, 25(9), 110-122.

Haris, M., Yao, H., & Fatima, H. (2024). The impact of liquidity risk and credit risk on bank profitability during COVID-19. *Plos one*, *19*(9), e0308356.

Harunurrasyid, H., Gustriani, G., Mardalena, M., & Nida, R. (2024). The impact of digital transformation on financial inclusion: Evidence from MSMEs in Indonesia. *Jurnal Perspektif Pembiayaan dan Pembangunan Daerah*, *12*(4), 343-356.

Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F. J., & Urueña, A. (2021). Smartphone addiction and cybercrime victimization in the context of lifestyles routine activities and self-control theories: The user's dual vulnerability model of cybercrime victimization. *International journal of environmental research and public health*, *18*(7), 3763.

Hudson, R., & Maioli, S. (2010). A response to "Reflections on a global financial crisis". *Critical perspectives on international business*, *6*(1), 53-71.

Ibekwe, A. O. (2021). Financial innovation and performance of deposit money banks in Nigeria. *International Journal of Business & Law Research*, *9*(1), 162-173.

Idolor, E. J. (2010). Bank frauds in Nigeria: Underlying causes, effects and possible remedies. *African journal of accounting, economics, finance and banking research*, *6*(6), 62.

Idowu, A., Adedipe, O. A., & Aderoju, A. (2022). Internal control system and corporate survival in the Nigerian banking sector: The mediatory role of ethical climate. *ACU Journal of Social and Management Sciences*, 2(1), 162-178.

Islam, M. T., Islam, M. F., & Sawda, J. (2022). E-commerce and cyber vulnerabilities in bangladesh: A policy paper. *International Journal of Law and Society*, *1*(3), 186-203.

Jacobson, D., & Idziorek, J. (2012). *Computer security literacy: Staying safe in a digital world*. CRC Press.

John, O. A., & Rotimi, O. (2014). Analysis of electronic banking and customer satisfaction in Nigeria. *European journal of business and social sciences*, *3*(3), 14-27.

Kanoujiya, J., Bhimavarapu, V. M., & Rastogi, S. (2023). Banks in India: a balancing act between profitability, regulation and NPA. *Vision*, *27*(5), 650-660.

Ketron, S., & Naletelich, K. (2016). How e-readers have changed personal connections with books. *Qualitative market research: An international journal*, *19*(4), 433-452.

Khalil, K. (2020). Effect of cyber security costs on performance of E-banking in Pakistan. *Journal of Managerial Sciences*, *14*(4), 85-99.

Klimburg, A. (2011a). Mobilising cyber power. *Survival*, 53(1), 41-60. doi:10.1080/00396338.2011.555595

Klimburg, A. (2011b). The Whole of Nation in Cyberpower. *Georgetown Journal of International Affairs*, 171–179.

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance*, *19*(6), 466-492.4

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior*, *126*, 106979.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Limnéll, J., Majewski, K., & Salminen, M. (2015). Cyber security for decision makers. Jyväskylä, Finland: Docendo.

Makanga, F. I. (2021). *An Assessment of the Implementation of Free Movement of Persons in East Africa Community-a Case of Kenya* (Doctoral dissertation, University of Nairobi).

McQuade, B. (2019). *Pacifying the homeland: Intelligence fusion and mass supervision*. Univ of California Press.

Mohamed Abdel Razek Youssef, A. (2022). The Role of the Digital Economy in Sustainable Development. *International Journal of Humanities and Language Research*, *5*(2), 13-25.

Mohamed Mizan, N. S., Ma'arif, M. Y., Mohd Satar, N. S., & Shahar, S. M. (2019). CNDS-cybersecurity: issues and challenges in ASEAN countries. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(1.4).

Morah, D. N., & Uzochukwu, C. E. (2019). Nigeria's social media culture: exploring civic participation of youths in the 2015 Presidential Election. *International Journal of Advance Study and Research Work*, *2*(1), 1-12.

Muchiri, C. W., & Muathe, S. M. (2024). Strategic orientation and organizational performance: evidence from rotary clubs in Kenya. *Journal of Business and Management Sciences*, *12*(2), 99-110.

Muhati, E. (2018). *Factors affecting cyber-security in Kenya–A Case of Small Medium Enterprises* (Doctoral dissertation, Strathmore University).

Njoku, C. U., Iwueke, O. C., & Emezi, C. N. (2023). Community Stakeholders Participation in Extractive Industry Corporate Social Responsibility. *Nigerian Academy of Management Journal*, *18*(1), 39-49.

Njoroge, A. W. (2020). *Intelligence aspects of big data analytics for Kenya national security* (Doctoral dissertation, Strathmore University).

Nugraha, R., & Bayunitri, B. I. (2020). The influence of internal control on fraud prevention (Case study at Bank BRI of Cimahi City). *International Journal of Financial, Accounting, and Management*, *2*(3), 199-211.\

Nugraha, R., & Bayunitri, B. I. (2020). The influence of internal control on fraud prevention (Case study at Bank BRI of Cimahi City). *International Journal of Financial, Accounting, and Management*, *2*(3), 199-211.

Nwarize, C. P. (2023). *An investigation of factors influencing non-users' resistance to internet banking adoption in Nigeria* (Doctoral dissertation, Cardiff Metropolitan University).

Nyirambyeyi, H. (2018). Automated teller machine system and service quality in commercial banks in Kigali, Rwanda.

Ogunwale, H. (2020). The impact of cybercrime on Nigeria's commercial banking system. *International Journal of Management and Business Studies*, *2*(3), 75-78.

Ojeka, S. A., Ben-Caleb, E., & Ekpe, E. O. I. (2017). Cyber security in the nigerian banking sector: an appraisal of audit committee effectiveness. *International Review of Management and Marketing*, *7*(2), 340-346.

Olaniran, O. (2022). *Success factors influencing cyber security risk management implementation: the cases of large Nigerian organisations* (Doctoral dissertation, Coventry University).

Omenazu, S. (2022). Strategic management, decision making and organizational performance: case study of construction industry Malaysia. *Journal of Positive School Psychology*, *6*(3), 6100-6113.

Onapajo, H., & Uzodike, U. O. (2014). Rigging through the courts: The judiciary and electoral fraud in Nigeria. *Journal of African Elections*, *13*(2), 137-168.

Oni, O. O. (2019). *Determinants of non-performing loans of deposit money banks in Sub-Saharan Africa* (Doctoral dissertation, Kwara State University (Nigeria)).4

Osi, E. U., Jerry, D. O., & Mark, E. B. (2024). Audit Committee Attributes and Financial Performance of Listed Oil and Gas Firms in Nigeria. *UMYU Journal of Accounting and Finance Research*, *6*(1), 120-139.

Otusanya, O. J. (2020). 5 The Role of Transparency, Internal Control and Risk Management in Corporate Governance: The Case of Nigeria. *African Management*, 87-122. Doi 10.1515/9783110629026-005

Otusanya, O. J., & Adeyeye, G. B. (2022). The dark side of tax havens in money laundering, capital flight and corruption in developing countries: some evidence from Nigeria. *Journal of Financial Crime*, *29*(1), 62-100.

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, *142*, 103744.

Ratzinger-Sakel, N. V., & Tiedemann, T. (2022). Fraud in accounting and audit research (1926–2019)–a bibliometric analysis. *Accounting History Review*, *32*(2-3), 97-143.

Renugadevi, P., Sudha, A., & Srimathi, R. (2024, August). A Case Study for Standalone Solar Power Modules with and Without IoT Devices in Rural Hospital Emergency Rooms Located inKaniyambadi. In *2024 IEEE International Communications Energy Conference (INTELEC)* (pp. 1-6). IEEE.

Reveron, D. S. (Ed.). (2012). *Cyberspace and national security: threats, opportunities, and power in a virtual world*. Georgetown University Press.

Rudasill, L., & Moyer, J. (2004). Cyber-security, cyber-attack, and the development of governmental response: the librarian's view. *New library world*, *105*(7/8), 248-255.

Shaker, A. S., Al Shiblawi, G. A. K., Union, A. H., & Hameedi, K. S. (2023). The role of information technology governance on enhancing cybersecurity and its reflection on investor confidence. *International Journal of Professional Business Review*, *8*(6), 7.

Singh, M. M., Frank, R., & Zainon, W. M. N. W. (2021). Cyber-criminology defense in pervasive environment: A study of cybercrimes in Malaysia. *Bulletin of Electrical Engineering and Informatics*, *10*(3), 1658-1668.

Singleton, T. W., & Singleton, A. J. (2010). *Fraud auditing and forensic accounting*. John Wiley & Sons.

Solansky, S. T., & Beck, T. (2021). Interorganizational information sharing: Collaboration during cybersecurity threats. *Public Administration Quarterly*, *45*(1), 105-122.

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future generation computer systems*, *92*, 178-188.

Sulaeman, H. S. F., Moelyono, S. M., & Nawir, J. (2019). Determinants of Banking Efficiency for Commercial Banks in Indonesia. *Contemporary Economics*, *13*(2), 205-218.

Suleiman, M. O. (2024). *Effective Strategies Leaders Use to Reduce Fraud in the Nigerian Banking Industry* (Doctoral dissertation, Walden University).

Thomas, E. O., Gbadeyan, R. O., & Waheed, I. (2023). Business Process Management Tools and Performance of Small and Medium Scale Enterprises in Lagos State, Nigeria. *African Journal of Management and Business Research*, *12*(1), 49-60.

Wada, F., & Odulaja, G. (2012). Assessing cybercrime and its impact on E-banking in Nigeria using social theories. African Journal of Computing ICTs, 4(2), 69-82.

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415.

Yar, H., Imran, A. S., Khan, Z. A., Sajjad, M., & Kastrati, Z. (2021). Towards smart home automation using IoT-enabled edge-computing paradigm. *Sensors*, *21*(14), 4932.

Yousuf, O., & Mir, R. N. (2019). A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures. *Information & Computer Security*, *27*(2), 292-323.

Abdulhameed Idris
Department of Business Administration, Faculty of Management Sciences
Nile University of Nigeria, Abuja
anateovaino@gmail.com

Frank Alaba Ogedengbe
Department of Business Administration
Faculty of Management Sciences
Nile University of Nigeria, Abuja
FCT, Nigeria
frank.ogedengbe@nileuniversity.edu.ng
ORCID: 0000-0001-8896-7352

Amal Altalhi
Claremont Graduate University
Information systems and Technology,
Claremont, CA, USA
amal.altalhi@cgu.edu
University of Tabuk
College of Business Administration,
Department of Management information Systems,
Tabuk, Saudi Arabia
aaltalhi@ut.edu.sa
ORCID: 0009-0006-6107-8620