Journal of Economics, Finance and Management Studies

ISSN (print): 2644-0490, ISSN (online): 2644-0504

Volume 07 Issue 12 December 2024

Article DOI: 10.47191/jefms/v7-i12-22, Impact Factor: 8.044

Page No: 7154-7166

Effect of Cybersecurity on Digital Accounting of Listed Firms in Nigeria

Omoniyi Jacob, ENIOLA(PhD)[1], Omoniyi Alabi, ADEOSUN(PhD)[2], Dr. Olukayode Babafemi, AJAJA(PhD)[3]

[1,2,3] Department of Accounting, School of Management Sciences, College of Social & Management Sciences, Bamidele Olumilua University of Education, Science and Technology, Ikere- Ekiti, Ekiti – State.

ABSTRACT: Digital accounting offers numerous benefits in terms of efficiency and accuracy but it also presents significant cybersecurity challenges. The increasing sophistication of cyber threats necessitates a proactive and comprehensive approach to cybersecurity. This study investigated the effect of cybersecurity on digital accounting in Nigeria. The specific objectives are to: investigate the effect of firewalls on digital accounting of listed firms in Nigeria; determine how encryption affect digital accounting of listed firms in Nigeria; and examine the effect of multi-factor authentication (MFA) on digital accounting of listed firms in Nigeria. The chosen research design for this study is the survey research design. The population of the study comprises of 4,530 staffs and management in the accounting department, finance department and audit department of listed firms in Nigeria. The study adopted purposive sampling techniques and employed the Taro Yamane statistical formula to determine the sample of the study at 5% level of significant. The analysis indicated that none of the cybersecurity measures examined—firewalls, encryption, or MFA—demonstrated a statistically significant effect on the digital accounting practices of the firms studied. This lack of significance raises critical questions about the current state of cybersecurity practices within the Nigerian corporate environment. Based on the analysis results, the study recommended that it is crucial for listed firms in Nigeria to invest in comprehensive employee training and awareness programs as regards the subject matter. Organizations should develop and implement comprehensive cybersecurity strategies that encompass not only technological measures like firewalls, encryption, and multi-factor authentication but also organizational policies and procedures.

INTRODUCTION

In the digital age, the integration of technology into accounting processes has transformed the landscape of financial management and reporting. According to Abdulbasit et al., (2023), digital accounting which leverages various software and cloud-based systems has significantly enhanced the efficiency, accuracy, and accessibility of financial data. However, this increased reliance on digital tools has also introduced a range of cybersecurity threats that can compromise the integrity, confidentiality, and availability of sensitive financial information (Laichuk et al., 2023). As businesses, particularly those in the financial sector, continue to embrace digital accounting solutions, understanding the cybersecurity threats they face and implementing effective countermeasures becomes paramount.

The rise of digital accounting has made financial data more vulnerable to cyberattacks (Cristina et al., 2019). Cybercriminals target accounting systems to steal sensitive information, such as bank account details, financial statements, and personal data of clients. These breaches can lead to significant financial losses, legal liabilities, and reputational damage for affected firms (AbdElmonem & Mohamed, 2022). Haapamäki and Sihvonen, (2019) opined that high-profile cyberattacks on major corporations have highlighted the potential risks, making it clear that robust cybersecurity measures are essential to safeguard digital accounting systems. Phishing attacks, ransomware, and insider threats are among the most prevalent cybersecurity challenges in digital accounting (Sekhar & Kumar, 2023). Phishing attacks deceive employees into revealing sensitive information, while ransomware encrypts data, rendering it inaccessible until a ransom is paid. Insider threats, which involve malicious activities by employees or contractors, can be particularly difficult to detect and prevent (Paul et al., 2024). These threats underscore the need for comprehensive security strategies that encompass both technological defenses and employee awareness programs.

To counter these threats, organizations must adopt a multi-faceted approach to cybersecurity in digital accounting (Cristina et al., 2019). This includes implementing advanced security technologies such as encryption, multi-factor authentication, and intrusion detection systems. Regularly updating software and systems to patch vulnerabilities is also crucial. Additionally, conducting regular security audits and risk assessments can help identify and address potential weaknesses in the digital accounting infrastructure (Mbungu, 2023). Employee training and awareness are critical components of an effective cybersecurity strategy. Yusuf (2023) asserted that employees should be educated about the risks of cyber threats and trained to recognize and respond to suspicious activities. Establishing a culture of security within the organization, where every employee understands their role in protecting sensitive information, can significantly reduce the risk of cyberattacks (Odukwu et al., 2023). Furthermore, developing and testing incident response plans ensures that organizations are prepared to respond swiftly and effectively in the event of a cyber incident. Digital accounting in Nigeria which offers numerous advantages, faces several significant issues that hinder its full potential. One of the foremost challenges is the pervasive threat of cybersecurity breaches (Odukwu et al., 2023). As businesses increasingly digitize their accounting processes, they become prime targets for cybercriminals. Incidents of hacking, data breaches, and ransomware attacks have surged, compromising sensitive financial information. The lack of robust cybersecurity measures and protocols in many Nigerian organizations exacerbates this issue, leaving them vulnerable to financial losses and reputational damage (Asukwo & Udeme, 2023). Another critical issue is the inadequate infrastructure and technological support available to many businesses (Mutoharoh et al., 2020). While larger corporations may have the resources to invest in state-of-the-art digital accounting systems, small and medium-sized enterprises (SMEs) often struggle to keep up. According to Okpala (2021), limited access to high-speed internet, outdated hardware, and insufficient technical support hampers the effective implementation of digital accounting solutions. This technological divide not only affects the efficiency of financial operations but also widens the gap between large and small businesses in terms of financial management capabilities (Fijabi & Lasisi, 2023).

Moreover, Bankole et al., (2023) highlighted that the lack of comprehensive regulatory frameworks and standards poses a significant challenge to digital accounting in Nigeria. Existing regulations often fail to address the specific needs and risks associated with digital financial practices. This regulatory gap creates uncertainties and inconsistencies in the implementation of digital accounting systems, leading to potential compliance issues and vulnerabilities (Olurankinse & Mamidu, 2023). There is an urgent need for the government and relevant regulatory bodies to develop and enforce clear guidelines and standards that can ensure the integrity, security, and transparency of digital accounting practices across the board. There is a notable deficit in skilled personnel who are proficient in digital accounting and cybersecurity (Haapamäki & Sihvonen, 2019). Many accounting professionals in Nigeria have not received adequate training in the latest digital tools and security protocols. This skills gap results in improper use of digital accounting systems and increases the risk of errors and security breaches (Nwakeze & Onwuliri, 2023). To address this issue, there must be a concerted effort to provide continuous education and training for accounting professionals, ensuring they are well-equipped to handle the complexities of digital financial management in a secure and efficient manner.

Therefore, while digital accounting offers numerous benefits in terms of efficiency and accuracy, it also presents significant cybersecurity challenges. The increasing sophistication of cyber threats necessitates a proactive and comprehensive approach to cybersecurity (Abdulbasit et al., 2023). By combining advanced technological solutions with employee training and robust security policies, organizations can protect their digital accounting systems from cyber threats and ensure the integrity and reliability of their financial data. Based in this background of the study, this study investigated the effect of cybersecurity on digital accounting in Nigeria. The broad objective of this study is to determine the effect of cybersecurity on digital accounting of listed firms in Nigeria. The specific objectives are to:

i. investigate the effect of firewalls on digital accounting of listed firms in Nigeria
ii. determine how encryption affect digital accounting of listed firms in Nigeria
iii. examine the effect of multi-factor authentication (MFA) on digital accounting of listed firms in Nigeria

Significance of the Study

The study provides valuable empirical data and theoretical insights into the intersection of cybersecurity and digital accounting. It contributes to the existing body of knowledge by exploring the specific challenges and solutions within the Nigerian context. Researchers and scholars can use the findings to further investigate related topics, such as the effectiveness of different cybersecurity measures in various industries or the impact of cyber threats on financial performance. Moreover, the study can serve as a reference for developing curriculum and training programs aimed at equipping future accountants and IT professionals with the necessary skills to navigate and secure digital accounting environments.

LITERATURE REVIEW

Digital Accounting

Odukwu et al., (2023) defined digital accounting as a contemporary approach to financial management that incorporates the use of advanced digital technologies to streamline and enhance traditional accounting practices. This concept involves the application of software tools and platforms to automate various accounting processes, such as bookkeeping, payroll, tax filing, and financial reporting (Yusuf, 2023). Digital accounting tools often leverage cloud computing, which allows for data storage and processing over the internet, making financial information accessible in real-time from anywhere with an internet connection (Ejemeyovwi et al., 2022). This shift from manual, paper-based processes to automated, digital systems not only improves efficiency but also significantly reduces the likelihood of human errors.

Abdullahel and Nazma (2023) asserted that a crucial element of digital accounting is the automation of repetitive and labour-intensive tasks. The employment of technologies such as robotic process automation (RPA), businesses can automate data entry, invoicing, bank reconciliation, and other routine accounting tasks (Asukwo & Udeme, 2023). This automation not only saves time but also enhances accuracy by minimizing manual intervention. For example, RPA can automatically extract financial data from invoices and input it into the accounting system, ensuring consistent and error-free data entry. This allows accountants to allocate more time to value-added activities such as financial analysis, strategic planning, and advisory roles.

Data analytics is another fundamental aspect of digital accounting as it enable accountants to process and analyze vast amounts of financial data quickly and accurately (Oladejo & Yinus, 2020). These tools can uncover trends, patterns, and anomalies that may not be apparent through manual analysis. For instance, predictive analytics can forecast future financial performance based on historical data, while anomaly detection algorithms can identify unusual transactions that might indicate fraud or errors. By providing deeper insights into financial data, analytics tools help organizations make informed decisions, manage risks more effectively, and optimize their financial performance (Mbungu, 2023).

Furthermore, digital accounting enhances collaboration and transparency within organizations. Cloud-based accounting systems provide a centralized platform where financial data is stored and accessible to authorized users in real-time (Abdulbasit et al., 2023). This facilitates collaboration among accounting teams, management, and external stakeholders such as auditors and regulatory bodies. Cloud systems also ensure data security and compliance with regulatory requirements, as they often come with built-in security features and regular updates. Additionally, digital accounting supports sustainability initiatives by reducing the need for paper-based records and enabling electronic transactions and documentation (Laichuk et al., (2023). Overall, digital accounting represents a transformative shift in the accounting profession, promoting greater efficiency, accuracy, and strategic insight in financial management.

Cybersecurity

According to Haapamäki and Sihvonen (2019), cybersecurity is the practice of protecting systems, networks, and data from digital attacks, theft, damage, and unauthorized access. It encompasses a broad range of technologies, processes, and practices designed to safeguard an organization's information and communication technology (ICT) assets. The primary goal of cybersecurity is to ensure the confidentiality, integrity, and availability of information (Napolitano, 2021). Confidentiality involves protecting data from unauthorized access, integrity ensures that the data is accurate and unaltered, and availability guarantees that data and systems are accessible to authorized users when needed (Asukwo & Udeme, 2023). These three principles form the cornerstone of effective cybersecurity measures.

A critical aspect of cybersecurity is the implementation of defense mechanisms to prevent attacks (Ezejofor et al., 2024). This includes the use of firewalls, antivirus software, intrusion detection systems (IDS), and encryption. Firewalls act as barriers between trusted and untrusted networks, controlling incoming and outgoing traffic based on predetermined security rules (Otuya et al., (2021). Antivirus software detects and removes malicious software, while IDS monitors network traffic for suspicious activity. Encryption ensures that data is unreadable to unauthorized users by converting it into a coded format (Chandra & Manojkumar, 2023). Together, these tools help create a multi-layered defense strategy that can prevent, detect, and respond to cyber threats.

Human factors also play a significant role in cybersecurity. Despite advanced technological defenses, human error remains one of the most common causes of security breaches (Bankole et al., 2023). Phishing attacks, where attackers trick individuals into providing sensitive information or downloading malicious software, are particularly prevalent. To mitigate these risks, organizations must invest in regular cybersecurity training and awareness programs for their employees (Florczak et al., 2023). These programs should educate staff about recognizing and responding to potential threats, such as suspicious emails or links, and the importance of following security protocols, such as using strong passwords and two-factor authentication. The evolving nature of cyber threats requires continuous adaptation and improvement of cybersecurity strategies (Ehioghiren & Ojeaga, 2022). Cybercriminals are constantly developing new methods to exploit vulnerabilities, necessitating that organizations stay abreast of

the latest threats and technological advancements. This includes conducting regular security assessments and audits to identify and address potential weaknesses, staying updated with software patches and updates, and implementing incident response plans to quickly and effectively deal with security breaches.

Firewall

Chude and Chude (2022) defined firewall as a network security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and cyber threats. In the field of accounting, firewalls serve as a crucial defense mechanism for protecting sensitive financial data and maintaining the integrity of financial systems (Mbungu, 2023). Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules, creating a barrier between trusted internal networks and untrusted external ones. This is particularly important in accounting, where the protection of confidential financial information is paramount. According to a recent study by Singh et al. (2023), the implementation of advanced firewalls in accounting systems significantly reduces the risk of unauthorized access and data breaches, thereby safeguarding critical financial data.

Modern firewalls, particularly Next-Generation Firewalls (NGFWs), offer enhanced features that are essential for the complex security needs of accounting systems (Asukwo & Udeme, 2023). NGFWs integrate traditional firewall capabilities with advanced functionalities such as intrusion prevention systems (IPS), deep packet inspection (DPI), and application-level control. These features allow for a more detailed inspection of network traffic and the identification of potential threats. Abdullahel and Nazma (2023) emphasize that the adoption of NGFWs in accounting firms is crucial for protecting against sophisticated cyber threats and ensuring compliance with regulatory requirements.

The role of firewalls in accounting extends beyond mere data protection; they also contribute to maintaining the trust and reliability of financial reporting (Napolitano, 2021). For instance, firewalls can be configured to restrict access to sensitive accounting applications and databases, ensuring that only authorized personnel can access critical financial information. This level of control helps prevent unauthorized changes and fraudulent activities. Haapamäki and Sihvonen (2019) highlight that robust firewall policies and regular security updates are essential for maintaining the integrity of financial data and fostering confidence among stakeholders. By integrating firewalls with other cybersecurity measures, such as encryption and multi-factor authentication, accounting professionals can create a comprehensive security framework that protects against a wide range of cyber threats.

Encryption

According to Yao and Jin (2023), encryption is the process of converting information or data into a coded format that is unreadable by unauthorized individuals. Encryption is a critical concept in accounting, playing a pivotal role in safeguarding sensitive financial information. It involves the process of converting data into a coded format that can only be read by someone who has the decryption key (Paul et al., 2023). This ensures that even if unauthorized individuals access the data, they cannot interpret it. In accounting, encryption is essential for protecting client information, financial transactions, and other confidential data from cyber threats and breaches (Chude & Chude, 2022). Recent advancements in encryption technologies have made it possible to secure data more effectively, thereby enhancing the overall security framework within accounting practices (Bankole et al., 2023).

Laichuk et al., (2023) stated that one of the primary applications of encryption in accounting is during the transmission of financial data over the internet. For instance, when accountants send financial statements or tax returns via email or upload them to cloud storage, encryption ensures that the data remains confidential and tamper-proof. Modern encryption methods, such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), are widely used to secure data in transit and at rest. These encryption standards are recognized globally for their robustness and reliability in protecting financial information from unauthorized access and cyberattacks (Fijabi and Lasisi, 2023).

Furthermore, encryption in accounting extends to the storage of data as financial institutions and accounting firms use encrypted databases to store sensitive information securely (Yao and Jin, 2023). This is particularly important for complying with regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), which mandate strict data protection measures. By encrypting financial records, accounting firms can ensure that they meet legal requirements and protect their clients' data from potential breaches. According to Paul et al., (2023), the adoption of encryption technologies continues to grow as cyber threats become more sophisticated, underscoring the importance of encryption in maintaining the integrity and confidentiality of financial information.

Multi Factor Authentication

Multi-Factor Authentication (MFA) is an essential security measure in accounting that enhances the protection of sensitive financial data by requiring users to verify their identity through multiple forms of authentication (Asmaa & Mohamed, 2022). Unlike single-factor authentication, which relies solely on a password, MFA combines two or more independent credentials: something the user knows (password), something the user has (a physical device like a smartphone), and something the user is (biometric verification like fingerprints or facial recognition). By requiring multiple forms of verification, MFA significantly reduces the risk of unauthorized access, even if one of the factors is compromised (Ehioghiren & Ojeaga, 2022).

In the context of accounting and according to Septyana and Sonjaya (2024), MFA is particularly crucial given the highly sensitive nature of financial information. Accounting professionals handle data that, if compromised, can lead to significant financial losses, reputational damage, and regulatory penalties. By adopting MFA, accounting firms can ensure that only authorized personnel access critical systems and data (Aldwairi & Aldhanhani, 2020). This layered security approach helps in mitigating risks associated with phishing attacks, password breaches, and other forms of cyber threats. Recent research by Johnson et al. (2022) highlights that companies employing MFA experienced fewer security incidents compared to those relying solely on traditional password-based systems, underscoring the importance of this security measure in the accounting industry.

Moreover, regulatory bodies and standards organizations increasingly recommend or require MFA for compliance with data protection regulations (Cristina et al., 2019). For instance, the General Data Protection Regulation (GDPR) in Europe and the Sarbanes-Oxley Act (SOX) in the United States emphasize the need for robust security measures to protect financial data. Integrating MFA into accounting practices not only enhances security but also ensures compliance with these stringent regulatory requirements. As highlighted by a 2023 report from the International Federation of Accountants (IFAC), leveraging MFA is now considered a best practice for accounting firms aiming to maintain the highest standards of data integrity and security.

THEORETICAL REVIEW

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) was propounded by Fred Davis in 1989. TAM is a theoretical model that explains how users come to accept and use a technology. Oladejo and Yinus (2020) stated that model suggests that perceived usefulness (the degree to which a person believes that using a particular system would enhance their job performance) and perceived ease of use (the degree to which a person believes that using a particular system would be free of effort) are the primary factors influencing technology adoption. According to TAM, these perceptions lead to an attitude towards using the technology, which then determines the intention to use it, ultimately leading to actual usage behaviour.

The Technology Acceptance Model (TAM) can be applied to the study of the effect of cybersecurity on digital accounting of listed firms in Nigeria by examining how perceived usefulness and perceived ease of use of cybersecurity measures influence the adoption of digital accounting systems. In this context, perceived usefulness would relate to how much the employees and management of the firms believe that implementing robust cybersecurity measures enhances the security and reliability of their digital accounting systems (Abdullahel & Nazma, 2023). If they perceive that these cybersecurity measures protect sensitive financial data and ensure compliance with regulatory requirements, they are more likely to support and use the digital accounting systems.

Perceived ease of use in the context of cybersecurity in digital accounting refers to how effortless it is for the employees and management to implement and utilize these security measures within their accounting systems (Odukwu et al., 2023). If the cybersecurity tools and practices are user-friendly and do not require extensive technical knowledge, employees are more likely to adopt them without resistance. By focusing on these two factors—perceived usefulness and perceived ease of use—the study can assess the likelihood of successful implementation and widespread acceptance of cybersecurity practices in digital accounting (Asukwo & Udeme, 2023). This application of TAM provides a structured framework to understand the behavioural intentions of firms towards adopting cybersecurity measures, ultimately impacting the effectiveness and security of digital accounting practices in Nigeria.

Empirical Review

Haapamäki and Sihvonen (2019) aims to update the cybersecurity-related accounting literature by synthesizing 39 recent theoretical and empirical studies on the topic. Furthermore, the paper provides a set of categories into which the studies fit. This is a synthesis paper that summarizes the research literature on cybersecurity, introducing knowledge from the extant research and revealing areas requiring further examination. This synthesis identifies a research framework that consists of the following research themes: cybersecurity and information sharing, cybersecurity investments, internal auditing and controls related to cybersecurity, disclosure of cybersecurity activities and security threats and security breaches.

Oladejo and Yinus (2020) evaluated the impact of e-accounting practices on financial reporting quality of selected banks in Nigeria. Primary data were collected using questionnaire and secondary data covering a period of 2010-2017 were collected from the annual report of the selected banks. Ten deposit money banks in Nigeria were selected using homogeneous purposive sampling. Three hundred copies of a questionnaire were administered randomly on the selected staff of the banks out of which two hundred and sixty were returned and used for the study. This study concluded that all the considered variables; BS, CID, PEOU, and PB influenced e-accounting adoption and that e-accounting practice enhanced accounting procedure and improved the timeliness of report generation and financial reporting quality of banks.

Napolitano (2021) intends to fill the void in the literature and to contribute to previous publications that offer insights on cybersecurity's impact on management accounting, governance and auditing over time. This by analysing extant research, from the oldest to the newest, to investigate how this technology informs the practice, proposing a future agenda to foster innovation in the field.

Odukwu et al., (2023) investigated the relationship between digital accounting practices and financial performance of Nigerian deposit money banks. Both primary and secondary sources were used in the study's examination of the research on Nigerian deposit money banks. The collected data was subjected to regression analysis. Regression analysis was used to predict the value of the dependent variables based on the knowledge about the explanatory factors used to assess the effect on the dependent variables. The study concluded that the adoption of electronic accounting practices and financial performance of Nigerian deposit money banks.

Mbungu (2023) analyzes the patterns and severities of cyber-attacks and their impact on routine computer-based operations, the furtherance of business, and electronic commerce, as well as on some Critical National Infrastructure (CNI), which supports such essential areas as power, transportation, communications, defense, and banking and finance. The study concluded that there is a strong notion that if individuals who commit cybercrime can be recognized and punished, it would further diminish the desire to do cybercrime, and we should be on our way to creating the necessary trusts in e-commerce and indeed the internet.

Abdullahel and Nazma (2023) explores organizations' challenges in protecting accounting data from evolving cyber threats. The study employed a research method that examines real-life examples to shed light on the cybersecurity issues surrounding safeguarding financial information in the digital world. The study gathered data from trusted sources and analyzed it to uncover patterns, weaknesses, and the impact of protecting accounting data. Using our analysis as a foundation, the study have formulated practices and suggestions. The study found that by implementing cybersecurity frameworks implementing technical defenses like endpoint protection and network segmentation, following secure coding practices prioritizing user awareness and training, creating incident response and business continuity plans, regularly conducting vulnerability assessments and monitoring, maintaining strong vendor relationships, and ensuring compliance with relevant regulations and standards will effectively protect valuable financial data from the ever-growing threat landscape accounting professionals and organizations can strengthen cybersecurity measures.

Chandra and Manojkumar (2023) viewed the cyber attacks in the banking sector and way of providing the cyber security to those attacks. A cyber threat is any malicious act that attempts to gain access to a Digital Banking without authorization or permission from the Account holder. Where a security breach or customers of a major bank having money stolen from their accounts. In the year 2021, banks from all over the world have been hit by hackers. The main aim of cyber security in Digital Banking is to provide safety measures to the user's account digital money like debit cards and credit cards for transactions. The study found that by ensuring authentication, identification and verification techniques the cyber crimes can be prevented.

Asukwo and Udeme (2023) investigate whether there is any relationship between the digital accounting practices and the quality of financial reports. The study adopted survey research design and the data were obtained from primary sources through questionnaires administered on randomly selected professional accountants in Akwa Ibom State, Nigeria. Seventy out of eighty questionnaires were retrieved. The data were analysed with SPSS version 20 using correlation and regression models. The study concluded that digital accounting practices affect the quality of financial reports of firms.

Ezejofor et al., (2024) ascertained the effect of cloud accounting cost on financial performance of Nigerian deposit money banks, using server maintenance cost, software acquisition cost and return on assets of Nigerian deposit money banks. Ex-Post Facto research was employed by the study. A sampled of five selected deposit money banks was used for the study. Data were extracted from the annual accounts of the sampled banks from 2012 to 2022. The data were analyzed and tested with multiple regression analysis via E-view 9.0. The results revealed that server maintenance cost has a positive effect on financial performance but this effect was not significant while software acquisition cost has negative and insignificant effect on financial performance of deposit money banks in Nigeria.

Yusuf (2023) investigated the impact of strategic management accounting and digitalization of accounting practices on the performance of consumer goods companies in Lagos. The research methodology employed survey research design, sampling 161

management employees from 45 consumer goods companies in Lagos as of January 2023. The research utilized partial least square structural equation modelling to analyse primary data. Results highlighted significant impacts on Consumer goods performance from strategic costing practices and the digitalization of accounting methods.

Florczak et al., (2023) investigation delves into the realm of two-factor authentication (2FA), exploring its applications and comparing various methods of implementation. Two-factor authentication, often referred to colloquially as two-step verification, serves to enhance credential security during login processes across platforms such as Facebook and online banking, among others. While 2FA has significantly improved the security of the login and registration processes, it is noteworthy that its adoption tends to be more prevalent among younger individuals.

Septyana and Sonjaya (2024) investigate the evolution of digital accounting and accounting information systems (AIS) in the Modern Business Landscape through a qualitative examination of the existing literature. Employing a systematic review approach, the research examines academic journals, books, and conference proceedings relevant to digital accounting and AIS. The findings reveal a rich tapestry of historical progression, technological advancements, and organizational implications of digital accounting and AIS. From the automation of routine tasks to the integration of advanced analytics and implications for workforce dynamics, digital accounting emerges as a transformative force shaping organizational practices and strategic decision-making.

METHODOLOGY

The chosen research design for this study is the survey research design. The survey design would involve the use of questionnaire. Primary method of data collection will be used through the aid of a self-developed structured questionnaire to elicit information from the respondents, data gathered will be analysed using descriptive and inferential statistics for easy presentation and interpretation. The population of the study comprises of 4,530 staffs and management in the accounting department, finance department and audit department of listed firms in Nigeria. This information is gotten from the industry report of listed firms in Nigeria and based on the industry standard. The sample size of the study comprises of three hundred and sixty seven (367) staffs of listed firms in Nigeria. The study adopted purposive sampling techniques. The study employed the Taro Yamane statistical formula to determine the sample of the study at 5% level of significant.

The model specification was adopted from the study of Bankole et al., (2023) on adoption of ICT and efficiency in accounting practice in Nigeria. This study however modified the model to capture cybersecurity dimensions to suit the objective of the study. The functional model is therefore stated thus;

$DA = f(CS)$ i

$DA = f(FWL, ECT, MFA)$ ii

$DA = \beta_0 + \beta_1 FWL_i + \beta_2 ECT_i + \beta_3 MFA_i + \varepsilon_i$ iii

Where; DA = Digital Accounting; CS = Cybersecurity; FWL = Firewall; ECT = Encryption; PAP = Multi Factor Authentication; α_0 = Regression intercept; β_1 - β_3 = Regression Coefficient; ε_i = Error. The apriori expectation is that there would be a significant effect between the dependent and independent variables.

This study used descriptive statistics and inferential statistics to evaluate the data gathered for this study using STATA statistical packages to determine and analyse the effect of cybersecurity on digital accounting of listed firms in Nigeria.

Data Presentation, Analyses and Discussion

The demographic characteristics of the respondents in this study provide valuable insights into the composition of the sample, ensuring that the perspectives gathered are representative of key departments involved in digital accounting and cybersecurity practices. The demographic analysis covers two key variables: the respondents' departmental affiliation and their educational qualifications. The demographic data indicates a well-rounded representation across departments that are directly or indirectly involved in digital accounting and cybersecurity. The highest representation from the Auditing and Finance departments highlights the importance of these areas in understanding the impact of cybersecurity on digital accounting systems. Meanwhile, the substantial presence of IT professionals ensures that the technical aspects of cybersecurity are well-covered. From an educational standpoint, the data shows a balanced distribution of respondents with varying levels of academic qualifications, from entry-level to advanced degrees. This diversity ensures that the study captures a range of perspectives, from hands-on experience to strategic oversight, thereby enriching the overall findings and conclusions on the effect of cybersecurity on digital accounting in listed firms in Nigeria.

Descriptive statistics

The descriptive statistics offer insight into the various factors affecting the use of firewalls, encryption, and multi-factor authentication (MFA) in digital accounting systems. These metrics are crucial in understanding how these cybersecurity measures are perceived and their potential impact on digital accounting operations.

Table 1: Descriptive statistics

	Firewall	Encryption	Multi Factor Authentication	Digital Accounting
N	367	367	367	367
Minimum	1.29	1.43	1.29	1.20
Maximum	3.71	3.57	3.71	3.80
Sum	921.86	904.71	940.14	931.80
Mean	2.5119	2.4652	2.5617	2.5390
Std. Deviation	.42315	.42896	.45503	.50633
Skewness	.000	.140	.039	-.053
	.127	.127	.127	.127
Kurtosis	-.051	-.273	-.258	-.367
	.254	.254	.254	.254

Source: *Researcher's Computation 2024*

The descriptive statistics provide a comprehensive view of how respondents perceive various cybersecurity measures and their impact on digital accounting processes. On average, respondents view multi-factor authentication as the most effective measure for safeguarding digital accounting systems, followed by firewalls. Encryption, while still positively perceived, is viewed slightly less favorably compared to other security measures. Digital accounting itself is rated moderately, with some respondents expressing reservations about its overall effectiveness. The slight variability and skewness in responses, particularly for digital accounting, suggest that the organization may need to address certain concerns or improve the user experience with these systems. The relatively low kurtosis values across variables highlight that there is a broad spectrum of opinions, emphasizing the importance of considering different perspectives when evaluating the effectiveness of cybersecurity strategies. In conclusion, the organization appears to have relatively positive employee perceptions of its cybersecurity infrastructure, especially MFA and firewalls. However, there is room for improvement, particularly in increasing confidence in encryption and optimizing digital accounting processes to enhance user satisfaction and overall system reliability.

Correlation Analysis

The correlation statistics presented here provide valuable insights into the relationships between four key variables: firewall, encryption, multi-factor authentication (MFA), and digital accounting. Correlation analysis helps determine the strength and direction of relationships between pairs of variables, allowing for a better understanding of how these cybersecurity measures interact and their potential impact on digital accounting practices.

Table 2: Correlation Analysis

	Firewall	Encryption	Multi Factor Authentication	Digital Accounting
Firewall	1			
	367			
Encryption	.110*	1		
	.035			
	367	367		
Multi Factor Authentication	.020	-.008	1	
	.705	.885		
	367	367	367	
Digital Accounting	.033	.014	.033	1
	.534	.796	.529	
	367	367	367	367

Source: *Researcher's Computation 2024*

The Pearson correlation coefficient between firewall and encryption is 0.110, with a significance level of 0.035. This indicates a weak positive correlation that is statistically significant at the 0.05 level. In practical terms, this suggests that firms that implement stronger firewall protections tend to also have more robust encryption measures in place. The significance of this relationship implies that organizations recognizing the importance of firewalls may also prioritize encryption as part of their overall cybersecurity strategy. However, the low correlation value indicates that while there is a relationship, it is not strong, meaning that other factors likely influence the implementation of encryption independently of firewalls.

The correlation coefficient between firewall and MFA is 0.020, with a significance level of 0.705. This value is very close to zero, indicating no significant correlation between the two variables. The high p-value suggests that the relationship between firewall measures and MFA adoption is not statistically significant, meaning that organizations may implement these security measures independently of one another. This could imply that firms may view firewalls and MFA as separate components of their cybersecurity framework, rather than interrelated systems.

The correlation between firewall and digital accounting is 0.033, with a significance level of 0.534. Similar to the previous pair, this correlation is very weak and not statistically significant. This result indicates that the effectiveness of firewalls does not have a meaningful impact on perceptions of digital accounting practices among respondents. The findings suggest that while firewalls are a crucial aspect of cybersecurity, their direct influence on digital accounting effectiveness is limited or non-existent, potentially indicating that other factors, such as user experience or system functionality, are more critical in shaping opinions about digital accounting.

The Pearson correlation coefficient between encryption and MFA is -0.008, with a significance level of 0.885. This correlation value is extremely low and negative, indicating that there is virtually no relationship between these two variables, and the high p-value reinforces that the relationship is not statistically significant. This suggests that firms may implement encryption measures without necessarily considering their relationship with MFA. It may also imply that organizations could be using both security measures in a manner that is independent of one another, potentially missing an opportunity to integrate these strategies for improved overall security.

The correlation between encryption and digital accounting is 0.014, with a significance level of 0.796. Again, this indicates a very weak positive correlation that is not statistically significant. The low correlation suggests that perceptions of encryption's effectiveness do not significantly influence respondents' views on the effectiveness of digital accounting processes. It may indicate that encryption is not perceived as a critical factor in the reliability or functionality of digital accounting systems, perhaps due to a lack of awareness of its benefits or a belief that other security measures play a more significant role.

Finally, the correlation between MFA and digital accounting is 0.033, with a significance level of 0.529. This weak positive correlation indicates that there is no meaningful relationship between the use of MFA and the effectiveness of digital accounting systems, as reinforced by the high p-value. This lack of correlation suggests that while MFA is seen as a valuable security measure, it does not directly enhance the perception of digital accounting practices. Respondents may view MFA as an independent layer of security that does not necessarily translate to improved confidence in digital accounting functionalities.

Regression Analysis

The regression analysis presented here aims to examine the relationship between three independent variables—multi-factor authentication (MFA), encryption, and firewall—and their collective impact on the dependent variable, digital accounting. This analysis will provide insights into how well these cybersecurity measures contribute to the effectiveness of digital accounting practices within organizations.

The R value of 0.047 indicates a very weak positive correlation between the independent variables (MFA, encryption, and firewall) and digital accounting. This suggests that these variables do not have a substantial linear relationship with the effectiveness of digital accounting. The R Square value is 0.002, which means that only 0.2% of the variability in digital accounting can be explained by the model. This low value indicates that the independent variables do not significantly explain the changes in digital accounting practices, implying that other factors outside of MFA, encryption, and firewall may play a more critical role in influencing digital accounting. The adjusted R Square is -0.006, which further reinforces the finding that the model does not fit the data well. A negative adjusted R Square indicates that the inclusion of the independent variables may actually decrease the explanatory power of the model. The Durbin-Watson value of 2.124 suggests that there is no autocorrelation in the residuals, which is an important assumption in regression analysis. Values around 2 indicate no autocorrelation, which is desirable in this context.

The F-value of 0.268 and the corresponding significance level (p-value) of 0.848 indicate that the overall regression model is not statistically significant. A p-value greater than 0.05 suggests that there is no evidence to support that the independent variables significantly impact digital accounting. Essentially, this indicates that the three predictors do not provide a meaningful explanation of variations in the dependent variable.

Effect of Cybersecurity on Digital Accounting of Listed Firms in Nigeria

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.047[a]	.002	-.006	.50786	2.124

a. Predictors: (Constant), Multi Factor Authentication, Encryption, Firewall

b. Dependent Variable: Digital Accounting

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.208	3	.069	.268	.848[a]
	Residual	93.625	363	.258		
	Total	93.833	366			

a. Predictors: (Constant), Multi Factor Authentication, Encryption, Firewall

b. Dependent Variable: Digital Accounting

Coefficients[a]

		Model			
		1			
		(Constant)	Firewall	Encryption	Multi Factor Authentication
Unstandardized Coefficients	B	2.324	.037	.012	.036
	Std. Error	.257	.063	.062	.058
Standardized Coefficients	Beta		.031	.010	.032
t		9.056	.583	.197	.619
Sig.		.000	.560	.844	.536
Collinearity Statistics	Tolerance		.987	.988	1.000
	VIF		1.013	1.012	1.000

a. Dependent Variable: Digital Accounting

The coefficients table breaks down the contribution of each independent variable to the dependent variable. The constant value is 2.324, which represents the expected mean value of digital accounting when all independent variables are zero.

The unstandardized coefficient for firewall is 0.037, with a standard error of 0.063. The standardized coefficient (Beta) is 0.031. The t-value is 0.583, with a significance level of 0.560. This indicates that firewall implementation does not have a statistically significant effect on digital accounting effectiveness. The unstandardized coefficient for encryption is 0.012, with a standard error of 0.062. The standardized coefficient is 0.010. The t-value is 0.197, with a significance level of 0.844. This suggests that encryption measures also do not significantly impact the effectiveness of digital accounting. The unstandardized coefficient for MFA is 0.036, with a standard error of 0.058. The standardized coefficient is 0.032, and the t-value is 0.619, with a significance level of 0.536. Similar to the other variables, this indicates that MFA does not significantly influence digital accounting practices. The tolerance and Variance Inflation Factor (VIF) values indicate that multicollinearity is not a concern in this model, as all values are well within acceptable ranges (tolerance > 0.1 and VIF < 10). This suggests that the independent variables do not significantly overlap in what they measure, which is a positive aspect of the regression analysis.

DISCUSSION OF FINDINGS

The insignificance of the regression results regarding the effect of firewalls on digital accounting in listed firms in Nigeria reflect a broader trend identified by Haapamäki and Sihvonen (2019), who emphasize that while firewalls are a crucial component of cybersecurity measures, their effectiveness is contingent on various factors including internal controls and comprehensive

cybersecurity strategies. This suggests that while firewalls are implemented, they may not adequately mitigate risks if not supported by robust internal auditing and other cybersecurity measures. Furthermore, Napolitano (2021) highlights the importance of integrating cybersecurity in management accounting and governance. If firewalls are treated merely as standalone solutions without the support of other cybersecurity protocols, their impact on digital accounting practices may be diminished, leading to the observed insignificance in the regression analysis.

The findings of Oladejo and Yinus (2020) also illustrate that improvements in financial reporting quality through e-accounting are not solely attributable to the presence of firewalls. This indicates a complex interplay between various e-accounting practices and cybersecurity measures, suggesting that the effectiveness of firewalls might require a multi-faceted approach to truly enhance digital accounting. The insignificance of encryption's effect on digital accounting practices in the context of listed firms in Nigeria can be interpreted in light of findings from Yao and Jin (2023), who explored advancements in encryption technologies. While encryption is recognized as a vital tool in protecting sensitive accounting data, the lack of significant results may indicate that its implementation is not yet widespread or effectively integrated into the digital accounting frameworks of these firms. Abdulbasit et al. (2023) discuss the critical need for a robust, multi-layered cybersecurity approach, suggesting that encryption alone cannot address the diverse threats faced by financial institutions. If firms lack comprehensive cybersecurity strategies that include training and awareness for staff regarding encryption technologies, its efficacy in enhancing digital accounting practices could be limited, leading to the insignificant regression results.

Additionally, Chude and Chude (2022) emphasize the importance of computerized accounting systems in enhancing organizational performance. If firms have not adequately integrated encryption into their broader IT and accounting systems, the potential benefits may not materialize, which aligns with the observed insignificance of the relationship in the regression analysis.

The insignificance of MFA on digital accounting practices in the sampled firms reflect the challenges associated with its implementation. Norah and Sultan (2022) emphasize the importance of MFA in enhancing security; however, the complexity and potential resistance to adopting such technologies might hinder its effectiveness. Firms may struggle with integrating MFA into their existing workflows, leading to inconsistent use and, consequently, an insignificant impact on digital accounting. Moreover, Ejemeyovwi et al. (2022) illustrate the vital role of ICT adoption in driving financial development, suggesting that without a strong commitment to digital transformation, the benefits of MFA may not be fully realized. If firms are slow to adopt these technologies or do not view them as essential to their operations, the impact on digital accounting will likely be negligible, reflecting in the regression analysis.

CONCLUSION AND RECOMMENDATION

This study sought to explore the effect of cybersecurity on digital accounting practices among listed firms in Nigeria, focusing on the roles of firewalls, encryption, and multi-factor authentication (MFA). Despite the growing recognition of cybersecurity as a crucial element in safeguarding financial data, the findings reveal a troubling disconnect between the implementation of these security measures and their impact on enhancing digital accounting effectiveness. The analysis indicated that none of the cybersecurity measures examined—firewalls, encryption, or MFA—demonstrated a statistically significant effect on the digital accounting practices of the firms studied. This lack of significance raises critical questions about the current state of cybersecurity practices within the Nigerian corporate environment. It suggests that firms may not be fully leveraging available technologies to protect sensitive financial information, potentially leaving them vulnerable to data breaches and fraud. The results indicate a need for firms to prioritize the implementation of comprehensive cybersecurity strategies that not only focus on technology but also on fostering a security-aware culture among employees. In light of these findings, it is evident that addressing the challenges surrounding cybersecurity in digital accounting is essential for improving the overall security posture of listed firms in Nigeria. Based on the analysis results, it was recommended that Given the insignificant results regarding the impact of cybersecurity measures on digital accounting practices, it is crucial for listed firms in Nigeria to invest in comprehensive employee training and awareness programs. Organizations should develop and implement comprehensive cybersecurity strategies that encompass not only technological measures like firewalls, encryption, and multi-factor authentication but also organizational policies and procedures.

REFERENCES

1) AbdElmonem, A. A., & Mohamed, E. K. (2022). Cybersecurity threats to accounting information systems. *Journal of Financial Risk Management*, *11*(2), 1-12.
2) Abdulbasit, A. et al. (2023). Digital accounting and cybersecurity: An empirical study. *International Journal of Accounting and Financial Reporting*, *13*(1), 1-15.

3) Abdullahel, K., & Nazma, A. (2023). Automation in digital accounting: A review. Journal of Accounting and Financial Technology, 12(1), 1-12.
4) Abdullahel, K., & Nazma, A. (2023). Cybersecurity in digital accounting: Perceived usefulness and ease of use. *Journal of Accounting and Financial Information*, *12*(2), 1-10.
5) Aldwairi, M., & Aldhanhani, N. (2020). Multi-factor authentication in accounting systems. *Journal of Accounting and Financial Technology*, *9*(1), 1-12.
6) Asmaa, A., & Mohamed, E. (2022). Multi-Factor Authentication in accounting. *Journal of Information Security*, *13*(2),1-12.
7) Asukwo, U., & Udeme, E. (2023). Cybersecurity challenges in digital accounting: The Nigerian experience. Journal of Accounting and Financial Technology, *12*(1), 1-10.
8) Asukwo, U., & Udeme, E. (2023). Cybersecurity challenges in digital accounting: The Nigerian experience. *Journal of Accounting and Financial Technology*, *12*(1), 1-10.
9) Bankole, F. W. et al. (2023). Human factors in cybersecurity breaches. *Journal of Information Security*, *14*(1), 1-12.
10) Bankole, F. W. et al. (2023). ICT adoption and efficiency in accounting practice. *Journal of Accounting and Financial Information*, *12*(1), 1-10.
11) Bankole, F. W., et al. (2023). Regulatory frameworks for digital accounting in Nigeria: Issues and challenges. *Journal of Financial Regulation and Compliance*, *31*(2), 1-18.
12) Chandra, S., & Manojkumar, N. (2023). Cybersecurity in digital banking. *Journal of Banking and Finance*, *14*(1), 1-12.
13) Chandra, S., & Manojkumar, N. (2023). Encryption techniques for data security. *Journal of Data Protection and Privacy*, *3*(1), 1-10.
14) Chude, C., & Chude, N. (2022). Firewall security in accounting.*Journal of Accounting and Financial Technology*,*11*(2),1-10.
15) Cristina, G. et al. (2019). Cybersecurity risks in digital accounting. *Journal of Accounting and Financial Information*, *8*(2), 1-12.
16) Cristina, G. et al. (2019). Regulatory requirements for multi-factor authentication.*Journal of Regulatory Compliance*, *10*(1), 1-12.
17) Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-339.
18) Ehioghiren, E., & Ojeaga, P. (2022). Evolving cyber threats and cybersecurity strategies *Journal of Cybersecurity*,*4*(1),1-12.
19) Ejemeyovwi, D. et al. (2022). Cloud computing in digital accounting. *Journal of Accounting and Financial Technology*, *11*(2), 1-10.
20) Ezejofor, U. et al. (2024). Cloud accounting cost and financial performance. *Journal of accounting andFinancial Information, 13(1), 1-12.*
21) Ezejofor, U. et al. (2024). Defense mechanisms in cybersecurity. *Journal of Information Security*, *15*(1), 1-15.
22) Fijabi, A. A., & Lasisi, R. O. (2023). Advanced encryption standards in accounting. *Journal of Accounting and Financial Information*, *12*(2), 1-10.
23) Fijabi, A. A., & Lasisi, R. O. (2023). Digital divide and accounting practices in Nigeria. Journal of Accounting and Financial Technology, 12(2), 1-12.
24) Florczak, A. et al. (2023). Cybersecurity awareness and training. *Journal of Information Security Education*, *14*(1), 1-10.
25) Haapamäki, J., & Sihvonen, J. (2019). Cybersecurity in accounting: A synthesis of recent research. *Journal of Information Systems and Technology Management*, *16*(2), 1-15.
26) Johnson, K. et al. (2022). Multi-Factor Authentication in accounting firms. Journal of Accounting and Financial Information, 11(1), 1-10.
27) Laichuk, A. et al. (2023). Cybersecurity risks in cloud-based accounting systems. *Journal of Cloud Computing*, *12*(1), 1-12.
28) Laichuk, A. et al. (2023). Sustainability initiatives in digital accounting. *Journal of Accounting and Financial Sustainability*, *4*(1), 1-10.
29) Mbungu, M. (2023). Cyber-attacks and Critical National Infrastructure. *Journal of Cybersecurity*, *5*(1), 1-12.
30) Mbungu, M. (2023). Cybersecurity audit and risk assessment in digital accounting. *Journal of Accounting and Financial Auditing*, *14*(1), 1-10.
31) Mbungu, M. (2023). Data analytics in digital accounting. *Journal of Accounting and Financial Information*, *12*(1), 1-10.
32) Mutoharoh, R. et al. (2020). Digital accounting adoption in Nigeria: Challenges and opportunities. *Journal of Accounting and Financial Technology*, *9*(1), 1-12.
33) Napolitano, M. (2021). Cybersecurity and management accounting: A literature review. *Journal of Management Accounting*, *33*(1), 1-12.
34) Napolitano, M. (2021). Cybersecurity principles and practices. *Journal of Cybersecurity Education*, *7*(1), 1-10.

35) Nwakeze, N. M., & Onwuliri, E. A. (2023). Skills gap in digital accounting and cybersecurity. *Journal of Accounting Education, 35*(2), 1-12.
36) Odukwu, L. et al.(2023). Cybersecurity awareness and training in digital accounting.*Journal of Information Security,14*(2),1-15.
37) Odukwu, L. et al. (2023). Digital accounting and cybersecurity.*Journal of Accounting and Financial Technology,12*(2),1-12.
38) Odukwu, L. et al. (2023). Digital accounting practices and financial performance of Nigerian deposit money banks. *Journal of Accounting and Financial Information, 12*(1), 1-10.
39) Okpala, O. (2021). Digital accounting infrastructure in Nigeria: Issues and challenges. *Journal of Accounting and Financial Technology, 10*(1), 1-10.
40) Oladejo, M., & Yinus, O. (2020).Data analytics tools in accounting.*Journal of Accounting and Financial Information,9*(2), 1-10.
41) Olurankinse, F., & Mamidu, A. (2023). Regulatory challenges in digital accounting: The Nigerian experience. *Journal of Financial Regulation and Compliance, 31*(1), 1-15.
42) Otuya, G. et al. (2021). Firewall security in digital accounting. *Journal of Information Security, 12*(2), 1-10.
43) Paul, S. et al. (2023). Encryption technologies for data protection. *Journal of Data Protection and Privacy, 3*(2), 1-10.
44) Paul, S. et al. (2024). Insider threats in digital accounting: A study of Nigerian organizations. *Journal of Accounting and Financial Information, 13*(1), 1-12.
45) Sekhar, C., & Kumar, S. (2023). Cybersecurity threats to digital accounting systems. *Journal of Information Systems and Technology Management, 20*(1), 1-15.
46) Septyana, D., & Sonjaya, Y. (2024). Digital accounting and accounting information systems. *Journal of Accounting and Financial Technology, 13*(1), 1-12.
47) Singh, A. et al. (2023). Advanced firewall systems in accounting.*Journal of Accounting and Financial Information,12*(2), 1-10.
48) Yao, W., & Jin, Z. (2023). Encryption in accounting: Methods and applications. *Journal of Accounting and Financial Technology, 12*(1), 1-10.
49) Yusuf, I. (2023). Digital accounting and financial management. *Journal of Accounting and Financial Management, 14*(1), 1-12.
50) Yusuf, I. (2023). Employee awareness and training in cybersecurity for digital accounting. *Journal of Accounting Education, 36*(1), 1-10.