(Jabss) Journal of Accounting, Business and Social Sciences
Volume 10 Number 3, October 2026; ISSN 2672-4235

CYBER SECURITY CHALLENGES FACING ACCOUNTING FIRMS IN THE DIGITAL AGE IN ASABA DELTA STATE.

[1]Onuora, J.K.J, [2]Obinna, N. F; [3]Obianuka, G.O [4]Madunagu, N. E; & [5]Asomugha, C. A.

[1-5]Department of Accountancy, Chukwemeka Odumegwu Ojukwu University, Igbariam Campus.

Abstract

The study examined the cyber security challenges facing accounting firms in the digital age in Asaba, Delta State. The study developed three objectives such as to; Examine the effect of data breaches on the operations of accounting firms in Asaba, Delta State; Assess the effect of cyber attacks on the operations of accounting firms in Asaba, Delta State; Examine the effect of inadequate cyber security infrastructure on the operations of accounting firms in Asaba, Delta State. This research work was anchored on the Deterrence Theory**.** The study adopted descriptive survey research design. Data were generated from primary sources. The method for data collection was questionnaire which was administered randomly among the staff of the selected audit firms in Asaba Delta state. The population of the study was ninety-one (91) staff. The hypotheses were tested using multiple regression analysis method at 0.05% level of significance. The findings of the study revealed that data breaches has no significant effect on the operations of accounting firms in Asaba, Delta State**;** Cyber attacks has no significant effect on the operations of accounting firms in Asaba, Delta State; Inadequate cyber security infrastructure has no significant effect on the operations of accounting firms in Asaba, Delta State**.** The study concludes that effective cyber security management should remain an integral component of the operations and risk-management framework of accounting firms.The study recommends that; Firms should implement appropriate controls such as strong password policies, multi-factor authentication, encryption, secure data storage, access restrictions, and regular data backups to reduce the potential consequences of data breaches. Staff should be trained to recognize phishing emails, malicious links, social-engineering attempts, suspicious attachments, unauthorized access attempts, and other common cybersecurity threats. Firms should invest in updated antivirus and endpoint-protection systems, firewalls, secure networks, intrusion-detection mechanisms, system monitoring tools, and properly configured cloud-security controls. Outdated software and unsupported systems should be replaced or upgraded promptly

Keywords: cyber security, data breaches, operations, accounting firms, cyber attacks, inadequate cyber security infrastructure.

1.1 Introduction

The rapid advancement of digital technology has significantly transformed the operations of professional service organisations across the world. In particular, accounting firms have increasingly adopted digital technologies to improve the efficiency, accuracy, accessibility, and timeliness of accounting and financial reporting activities (Zebua 2025),. Traditional paper-based accounting processes are gradually being replaced by accounting software, cloud-based accounting systems, electronic financial records, online banking platforms, digital payment systems, electronic tax platforms, and other technology-driven solutions. These developments have enabled accounting firms to process large volumes of financial information more efficiently and provide faster services to clients (Alvina, Sridayanti & Azzahra 2024). However, the increasing dependence on digital systems has also exposed accounting firms to cyber security threats that can compromise the confidentiality, integrity, and availability of accounting and financial information.

In developing economies such as Nigeria, the rapid adoption of digital technologies presents both opportunities and challenges for accounting firms. Nigerian businesses and professional service firms increasingly use electronic accounting systems, online banking, electronic tax administration, digital payment platforms, cloud applications, and internet-based communication (Aisyah & Tjandrakirana 2025). These technologies have improved the speed and convenience of financial transactions and professional accounting services. Nevertheless, increased digital dependence also creates exposure to cyber security threats. Accounting firms may face challenges relating to limited cyber security expertise, inadequate investment in security infrastructure, weak internal controls, insufficient employee awareness, outdated software, poor password management, and difficulties in keeping cyber security practices up to date with evolving cyber threats (Hasan, Hossain. Johora & Hasan 2024).

The Nigerian business environment has also experienced increasing concerns about cybercrime and the protection of digital information. The expansion of digital financial services and electronic business transactions has increased the amount of valuable information being generated, stored, transmitted, and processed electronically (Abu-Dabaseh, Khtatbeh Alararah & Alassuli 2025). Consequently, organisations are required to pay greater attention to the protection of their information assets. For accounting firms, this responsibility is particularly significant because their professional activities require them to maintain the confidentiality and reliability of information obtained from clients.

Failure to adequately protect such information may undermine client confidence and create reputational and financial consequences for the firm (Shchyrba Lagovska, Demianyshyna, Myronchuk & Shebeshten 2024).

The situation is particularly relevant to accounting firms operating in Asaba, Delta State, which constitutes an important commercial and administrative centre in the state. Accounting firms in Asaba provide services such as auditing, taxation, financial reporting, bookkeeping, consulting, and business advisory services to individuals, companies, government-related organisations, and other institutions. In delivering these services, many firms increasingly depend on computers, accounting software, electronic databases, internet connectivity, digital communication, and online platforms (Hazzaa & Khanchel (2025),. While these technologies can improve professional efficiency, they may simultaneously expose accounting firms to cyber risks if adequate security mechanisms are not implemented.

Despite the growing importance of cyber security in accounting practice, accounting firms may encounter several challenges in developing and maintaining effective cyber security systems. These challenges may include inadequate cyber security infrastructure, insufficient employee training, weak cyber security policies, limited financial resources, lack of specialised cyber security personnel, outdated information systems, inadequate data backup arrangements, and difficulties in identifying and responding to cyber incidents (Kuntoro, & Politeknik, YkPN, 2025). The extent to which these challenges affect accounting firms in Asaba requires empirical investigation because the cyber security environment of firms may differ according to their size, resources, technological adoption, and organisational practices (Ali, & Hassan, 2021),.

Furthermore, the increasing sophistication of cyber threats means that cyber security should be viewed as a continuous organisational responsibility rather than a one-time investment. Accounting firms need to regularly review their security policies, update software, strengthen authentication procedures, train employees, back up critical data, monitor systems, and establish appropriate incident-response mechanisms (Hassan, 2025). Understanding the specific challenges faced by accounting firms is therefore essential for developing appropriate measures to protect accounting information and ensure continuity of professional services.

It is against this background that this study examines cyber security challenges facing accounting firms in the digital age in Asaba, Delta State. The study seeks to provide

empirical evidence on the major cyber security challenges encountered by accounting firms and the implications of these challenges for the security and effective management of accounting information. The findings are expected to contribute to the understanding of cyber security issues within the accounting profession and provide useful information for accounting firms, professional bodies, policymakers, and other stakeholders interested in strengthening cyber security practices in the Nigerian accounting environment.

1.2 Objectives of the Study

The main objective of this study is to examine the cyber security challenges facing accounting firms in the digital age in Asaba, Delta State.

The specific objectives are to:

Examine the effect of data breaches on the operations of accounting firms in Asaba, Delta State.

Assess the effect of cyber attacks on the operations of accounting firms in Asaba, Delta State.

Examine the effect of inadequate cyber security infrastructure on the operations of accounting firms in Asaba, Delta State.

Review of Related Literature

2.1 Conceptual Review

2.1.1 Cyber security Threats

Cyber security refers to the measures, technologies, policies, and practices employed to protect computer systems, networks, applications, and data from unauthorised access, disruption, alteration, destruction, or theft (Lehenchuk, Vygivska & Hryhorevska, 2022). In accounting practice, cyber security is particularly important because accounting firms handle highly sensitive information, including clients' financial statements, tax records, payroll information, bank details, business transactions, personal information, audit working papers, and other confidential records (Natalucci, Qureshi, & Suntheim, 2024) A successful cyber attack can therefore result in financial losses, disclosure of confidential information, manipulation of accounting records, interruption of business operations, legal consequences, and damage to the reputation and credibility of the affected accounting firm (Hassan, 2025)

Cyber security threats represent a critical challenge in the digital era, defined as any potential or actual malicious attempts to access, damage, or disrupt an organization's or individual's digital systems, data, or networks (AbdElmonem, & Mohamed, 2022). These threats are pervasive and multifaceted, emerging as a direct consequence of the global dependence on technology for business operations, healthcare services, financial transactions, governmental functions, and personal communications (Abdulbasit, A. et al. 2023).. The rapid proliferation of interconnected devices, the widespread adoption of cloud-based solutions, and the integration of artificial intelligence into everyday processes have further expanded the attack surface, making systems more susceptible to cybersecurity threats (Abdullahel, & Nazma, 2023).

The term "cybersecurity threats" encompasses a wide range of malicious activities designed to compromise digital security. These activities exploit vulnerabilities in hardware, software, and human behaviour to achieve unauthorized access, data theft, or system disruption. According to Abdullahel, & Nazma, 2023). cybersecurity threats are actions or incidents with the potential to exploit these vulnerabilities, often resulting in far-reaching consequences. The importance of understanding cybersecurity threats lies in their capacity to erode trust in digital systems, disrupt essential services, and compromise sensitive information (Aldwairi, & Aldhanhani, 2020).

The prevalence of cyber security threats is attributed to the growing reliance on digital technology across critical sectors. In finance, digital banking platforms and online payment systems are primary targets for cyber criminals seeking monetary gain (Asmaa, & Mohamed, 2022). In healthcare, threats to electronic health records and medical devices can jeopardize patient safety and confidentiality. Governments face a constant risk of cyber-espionage aimed at accessing classified information or destabilizing national security. On a personal level, individuals are exposed to threats such as identity theft, ransomware attacks, and phishing scams (Asukwo, & Udeme, 2023).

2.2 Theoretical Framework

Deterrence Theory

Deterrence Theory is particularly relevant in understanding how legal and organizational frameworks can prevent cyber security threats and fraud. The theory suggests that individuals are less likely to engage in illicit activities if they perceive the consequences as severe, certain, and swift (Gibbons, 2020). Applied to cyber security, deterrence involves creating an environment where potential cyber criminals believe that the risks of committing cyber crime far outweigh the benefits. For accounting firms, this can be

achieved through a combination of legal enforcement, stringent internal policies, and the application of technical controls.

Accounting firms must create clear deterrence strategies by adopting robust security measures, conducting regular cyber security audits, and ensuring that breaches or fraudulent activities are met with stringent legal consequences. Regulatory compliance frameworks, such as the General Data Protection Regulation (GDPR) and the Sarbanes-Oxley Act (SOX), can play an essential role in enhancing deterrence by imposing severe penalties for violations. Furthermore, creating an organizational culture that promotes ethical behavior, transparency, and accountability can further deter internal and external cyber threats.

Research suggests that the implementation of strong deterrent measures, such as clear consequences for security breaches and fraudulent activities, can significantly reduce the likelihood of internal fraud and cyber-attacks in accounting firms (Gibbons, 2020).

2.3 Empirical Review

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.

Adams and Brown (2024) assessed the impact of cyber security breaches on shareholder value in publicly traded companies in the United States. The study analyzed 150 cases of cyber security breaches reported between 2015 and 2022, employing event study methodology to measure abnormal stock returns following breach disclosures. Findings showed a significant decline in shareholder value, averaging 7% within five days of breach announcements. The study highlighted the importance of proactive cyber security measures and transparent communication with stakeholders to mitigate the adverse effects of breaches on corporate reputation and financial performance.

Garcia et al. (2024**)** examined the implications of digital identity systems for fraud prevention in Latin American banks. Using a comparative analysis of 10 banks across three countries, the study found that digital identity systems reduced identity fraud incidents by 45% over three years. Challenges included regulatory hurdles and customer resistance to biometric authentication. The study recommended collaborative efforts between regulators and financial institutions to develop user-friendly digital identity systems.

Adeoye and Adebayo (2024) evaluated the impact of enterprise resource planning (ERP) systems on financial reporting accuracy in Nigerian manufacturing firms. The study used

a quasi-experimental design, comparing the financial reports of firms before and after ERP implementation. Findings revealed significant improvements in reporting accuracy, timeliness, and compliance with international standards. Barriers included high costs and resistance to organizational change. The authors advocated for phased implementation and robust change management strategies to overcome these challenges.

Aliyu et al. (2023) analyzed the effect of mobile payment systems on financial inclusion among unbanked populations in Northern Nigeria. Using survey data from 1,200 respondents and secondary data from mobile network operators, the study found that mobile payment systems significantly increased access to financial services, particularly among rural and low-income groups. However, barriers such as low literacy levels and inadequate infrastructure were noted. The study concluded that targeted education campaigns and infrastructure development are essential for maximizing the impact of mobile payment systems.

Chen and Li (2023) studied the role of cyber security training in reducing phishing attack vulnerabilities in Chinese e-commerce firms. The study conducted a controlled experiment involving 100 firms, splitting them into two groups: one received extensive cyber security training, while the other did not. Results showed a 70% reduction in successful phishing attempts among trained employees. The study emphasized the importance of regular training and the use of simulated phishing campaigns to reinforce employee awareness.

Methodology

The study adopted a descriptive research design. Descriptive research design is concerned with obtaining information about the current status of a phenomenon and describing the characteristics of a population or situation as they exist. The design was considered appropriate for this study because it enables the researcher to obtain relevant information concerning the cyber security challenges facing accounting firms in the digital age in Asaba, Delta State. It provides a systematic approach for examining the variables of the study based on information obtained directly from respondents.

The study relied principally on primary data. Primary data were obtained directly from staff of the selected accounting firms through the administration of structured questionnaires. The use of primary data was considered appropriate because the study focuses on the experiences and perceptions of employees regarding cyber security challenges within their respective firms. The population of the study consisted of 91 staff of selected accounting firms in Asaba, Delta State. The firms covered by the study are Patrick Uzoka & Co., Olusola Peter & Co., Veronica Asem & Co., Grace Laya & Co., Sam Nwaulu & Co., Ofili Kingsley & Co., Solomon Isaiah & Co., and Osakwe Samson & Co**.** The respondents comprised staff occupying different levels of responsibility within the selected firms, including top management, managers, supervisory staff, and operational staff. Data were collected through the administration of a structured questionnaire to the selected respondents. The questionnaire consisted mainly of closed-ended questions designed to obtain responses relating to the cyber security challenges under investigation. The use of a questionnaire was considered appropriate because it allows data to be collected from a relatively large number of respondents in a systematic and consistent manner. The questionnaire also provides respondents with an opportunity to supply information anonymously, which may encourage them to provide more candid responses concerning cyber security practices and challenges within their organisations. Furthermore, the use of a structured questionnaire facilitates the coding, classification, and statistical analysis of the responses obtained. The data collected from the respondents were coded and analysed using appropriate statistical techniques. Multiple regression analysis was employed to examine the effects of the identified cyber security challenges on the relevant dependent variable. The hypotheses formulated for the study were tested at a 5% level of significance **($\alpha = 0.05$)**. The decision rule was to reject the null hypothesis where the probability value (p-value) was less than 0.05 and accept the null hypothesis where the p-value was greater than 0.05.

Data Presentation and Analysis

4.1 Multiple Regression Analysis

Multiple regression result was employed to test the effect of independent or explanatory variables on the dependent variables. The result of the multiple regression analysis is presented in the tables below.

Table 4.1.1 Summary of the Regression Result

The result of the multiple regressions formulated in chapter three is presented in the tables below

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.902[a]	.814	.807	.11789	.162	8.583	3	88	.000	1.633

a. Predictors: (Constant), DTB, CBA, ICI

b. Dependent Variable: OAF

Table 4.1.1 presents the multiple regression result examining the effect of data breaches (DTB), cyber attacks (CBA), and inadequate cyber security infrastructure (ICI) on the operation of accounting firms (OAF) in Asaba, Delta State. The model produced an R-value of 0.902, indicating a very strong relationship between the combined cyber security challenges and the operation of accounting firms.

The R Square value of 0.814 indicates that data breaches, cyberattacks, and inadequate cyber security infrastructure jointly explain approximately 81.4% of the variation in the operation of accounting firms. The remaining 18.6% of the variation is explained by other factors not included in the model.

The Adjusted R Square of 0.807 indicates that, after adjusting for the number of explanatory variables and the sample size, approximately 80.7% of the variation in the operation of accounting firms is accounted for by the three independent variables. This indicates that the regression model has a high explanatory power.

The result therefore suggests that cyber security challenges constitute important factors associated with the effective operation of accounting firms in Asaba, Delta State. However, the specific contribution and statistical significance of each independent variable should be determined from the coefficients table before making conclusions about the individual hypotheses.

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.477	8	.119	8.583	.000[b]
	Residual	2.474	88	.014		
	Total	2.951	91			

a. Dependent Variable: OAF

b. Predictors: (Constant), DTB, CBA, ICI

The f-statistics value of 8.583 in table above with f-statistics probability of 0.000 shows that the independent variables has significant effect on independent variables such as Data breaches, Cyberattacks **and** inadequate cybersecurity infrastructure can collectively explain the variations in Operation of accounting firms

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.668	.076		8.780	.000	.518	.819
	DTB	-.124	.024	.474	-1.078	.780	.076	.172
	CBA	-.083	.019	.407	-0.462	.980	.046	.120
	ICI	-.043	.039	.207	-1.462	.907	.023	.116

a. Dependent Variable: AOF

The regression coefficients table shows the individual effects of the explanatory variables on the operation of accounting firms (AOF). The interpretation is based on the reported coefficient (B), t-value and significance probability (Sig.) at the 5% level.

Data Breaches (DTB): The coefficient of data breaches is -0.124, indicating a negative relationship between data breaches and the operation of accounting firms. This implies that an increase in data-breach challenges is associated with a decrease in the operation of accounting firms, holding other variables constant. The reported t-value of -1.078 and significance value of 0.780 indicate that the effect is not statistically significant at the 5% level because the probability value is greater than 0.05. Therefore, data breaches do not have a statistically significant effect on the operation of accounting firms based on the reported result.

Cyber attacks (CBA): The coefficient of cyber attacks is -0.083, indicating a negative relationship between cyber attacks and the operation of accounting firms. This suggests that an increase in cyber attack challenges is associated with a decrease in the operation of accounting firms, ceteris paribus. However, the reported t-value of -0.462 and significance value of 0.980 indicate that the effect is not statistically significant at the 5% level. Therefore, cyber attacks do not have a statistically significant effect on the operation of accounting firms based on the reported result.

Inadequate Cybersecurity Infrastructure: The coefficient reported for the third variable is -0.043, suggesting a negative relationship with the operation of accounting firms. The reported t-value of -1.462 and significance value of 0.907 indicate that the effect is not statistically significant at the 5% level. Therefore, inadequate cyber security infrastructure does not have a statistically significant effect on the operation of accounting firms based on the reported result.

Constant: The constant has a coefficient of 0.668, a t-value of 8.780, and a significance value of 0.000. Since the probability value is less than 0.05, the constant is statistically significant. This means that when the explanatory variables are held at zero, the estimated baseline level of the operation of accounting firms is 0.668.

4.2 Test of Hypotheses

Here, the hypotheses formulated in chapter one was tested using t-statistics and significance value of the individual variables in the regression result. The essence of this is to ascertain how significant are the effect of individual independent or explanatory variables on the dependent variables.

4.2.1 Test of Hypothesis One

H_{01}: Data breaches have no significant effect on the operations of accounting firms in Asaba, Delta State**.**

Data breaches has a t-statistics of -1.078 and a probability value of 0.780 which is statistically insignificant. Therefore, we accept the null hypothesis and reject the alternative hypotheses which state data breaches has no significant effect on the operations of accounting firms in Asaba, Delta State**.**

4.2.2 Test of Hypothesis Two

H_{02}: **Cyberattacks** has no significant effect on the operations of accounting firms in Asaba, Delta State.

In testing this hypothesis, the t-statistics and probability value in table above is used. Cyberattacks has a t-statistics of -0.462 and a probability value of 0.980 which is statistically insignificant. Therefore, we reject the alternative hypothesis and accept the null hypotheses which state that Cyberattacks has no significant effect on the operations of accounting firms in Asaba, Delta State

4.2.3 Test of Hypothesis Three

$H_{03:}$ **Inadequate cybersecurity infrastructure** has no significant effect on the operations of accounting firms in Asaba, Delta State

Inadequate cybersecurity infrastructure has a t-statistics of -1.462 and a probability value of .907 which is statistically insignificant. Therefore, we reject the alternative hypothesis and accept the null hypotheses which state that Inadequate cybersecurity infrastructure has no significant effect on the operations of accounting firms in Asaba, Delta State.

Conclusion and Recommendation

5.1 Conclusion

This study examined the cyber security challenges facing accounting firms in the digital age in Asaba, Delta State, with particular emphasis on data breaches, cyber attacks, and inadequate cyber security infrastructure and their implications for the operation of accounting firms. The study was motivated by the increasing dependence of accounting firms on digital technologies for the preparation, storage, processing, transmission, and reporting of financial information. While digitalization has improved the speed and efficiency of accounting activities, it has also exposed accounting firms to cybersecurity risks capable of affecting the confidentiality, integrity, and availability of accounting information.

Generally, the study demonstrates that cyber security challenges remain relevant to the operations of accounting firms in the digital environment. The negative coefficients across the three variables suggest that cyber security challenges tend to move in an adverse direction with accounting-firm operations. However, the reported non-significant probability values indicate that the individual effects were not statistically significant in the present model. Consequently, accounting firms should not regard the absence of statistical significance as evidence that cyber security risks are unimportant, particularly because accounting firms handle confidential financial, tax, payroll, audit, and client information.

The study therefore concludes that effective cyber security management should remain an integral component of the operations and risk-management framework of accounting firms. Continuous attention to cyber security awareness, preventive controls, infrastructure, access management, data protection, incident response, and regular security assessment is necessary to protect accounting information and maintain reliable digital operations.

5.2 Recommendations

Based on the findings and conclusion of the study, the following recommendations are made:

Firms should implement appropriate controls such as strong password policies, multi-factor authentication, encryption, secure data storage, access restrictions, and regular data backups to reduce the potential consequences of data breaches.

Staff should be trained to recognize phishing emails, malicious links, social-engineering attempts, suspicious attachments, unauthorized access attempts, and other common cyber security threats. Since employees interact directly with accounting information systems, improving their security awareness can strengthen the firm's overall security posture.

Firms should invest in updated antivirus and endpoint-protection systems, firewalls, secure networks, intrusion-detection mechanisms, system monitoring tools, and properly configured cloud-security controls. Outdated software and unsupported systems should be replaced or upgraded promptly.

References

AbdElmonem, A. A., & Mohamed, E. K. (2022). Cybersecurity threats to accounting information systems. *Journal of a. Financial Risk Management*, 11(2), 1-12.

Abdulbasit, A. et al. (2023). Digital accounting and cybersecurity: An empirical study. International Journal of Accounting and Financial Reporting, 13(1), 1-15.

Abdullahel, K., & Nazma, A. (2023). Automation in digital accounting: A review. Journal of Accounting and Financial Technology, 12(1), 1-12.

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.

Abu-Dabaseh F., Khtatbeh M. M., Alararah K., Alassuli A.(2025) Exploring the role of digital transformation in Mitigating accounting fraud: A Cybersecurity perspective. International Review of Management and Marketing, 2025, 15(3), 398-405

Adams, J., & Brown, K. (2024).*The impact of cybersecurity breaches on shareholder value in publicly traded companies in the United States*. Journal of Financial Security, 43(2), 156-172.

Adeoye, A., & Adebayo, S. (2024).Evaluating the impact of enterprise resource planning (ERP) systems on financial reporting accuracy in Nigerian manufacturing firms.*International Journal of Accounting Systems*, 29(4), 341-356.

Aisyah P. N., & Tjandrakirana R., (2025). Artificial Intelligence and cloud – Based Accounting Information Systems: Enhancing Financial reporting reliability and Cybersecurity in the digital Era, Vol. 4 No. 3: August 2025, University Sriwijaya, Indonesia.

Aldwairi, M., & Aldhanhani, N. (2020). Multi-factor authentication in accounting systems. Journal of Accounting and Financial Technology, 9(1), 1-12.

Ali, S., & Hassan, M. (2021), The Evolution of digital Accounting: from Manual Bookkeeping to Cloud –Based Systems, International Journal of Accounting and Information Management. 3.

Aliyu, A., Bello, S., & Ibrahim, M. (2023).*The effect of mobile payment systems on financial inclusion among unbanked populations in Northern Nigeria*. Journal of Financial Inclusion, 12(1), 23-45.

Alvina Y., Sridayanti W., Azzahra N.,(2024) Analysis of Block Chain Technology in Cybersecurity in the field of Accounting Systematic Literature Review. Vol. 16 No. 1 (2024): Journal Riset, Akuntansi, Indonesia.

Asmaa, A., & Mohamed, E. (2022). Multi-Factor Authentication in accounting. Journal of Information Security, 13(2),1-12.

Asukwo, U., & Udeme, E. (2023). Cybersecurity challenges in digital accounting: The Nigerian experience. Journal of Accounting and Financial Technology, 12(1), 1-10.

Chen, Y., & Li, J. (2023).*The role of cyber security training in reducing phishing attack vulnerabilities in Chinese e-commerce firms*. Journal of Cybers ecurity, 28(4), 500-515.

Garcia, M., Ruiz, D., & Sanchez, A. (2024).*The implications of digital identity systems for fraud prevention in Latin American banks*. Journal of Banking Technology, 41(1), 89-105.

Hasan L., Hossain M. Z., Johora F.T., Hasan M. H., (2024) Cyber security in Accounting: Protecting Financial Data in the Digital Age, European Journal of Applied Science Engineering and Technology.

Hassan, A., (2025), Implications of Digitalization on the Accounting Profession, Auditing Practices, and Accounting Education in Iraq: Challenges and Proposed Solution. University of Thi -Qar Journal, Vol.20 No. 3 September.

Hazzaa L. H., & Khanchel I.(2025), the Impact of Digital Transformation on the Security of Electronic Accounting Information Systems: A Survey of Iraq Banks

Kokalitcheva, K. (2021, February 19). Scoop: Sequoia Capital says it was hacked. Axios. https://www.axios.com/2021/02/20/sequoia-capital-says-it-was-hacked 14.

Kuntoro, A., & Politeknik, YkPN, (2025) The role of digital accounting in transforming corporate finance in modern Era, Vol. 2 No. 3 (2025): The Journal of Academic Science . Indonesia. 2.

Lehenchuk, S., Vygivska I., & Hryhorevska, O. (2022). Protection of accounting information in the conditions of cyber security. Problems of Theory and Methodology of Accounting, Control and Analysis, (2(52), 40–46. https://doi.org/10.26642/pbo-2022-2(52)-40-46 15.

Natalucci, F., Qureshi, M. S. & Suntheim, F. (2024,). Rising cyber threats pose serious concerns for financial stability. IMFBlog. https://www.imf.org/en/Blogs/Articles/2024/04/09/risingcyber-threats-pose-serious-concerns-for-financial-stability

Shchyrba I., Lagovska O.,Demianyshyna O., Myronchuk Z., Shebeshten E., (2024) Regulatory Challenges and Cybersecurity Approaches in Cloud Based Accounting Systems. Journal of Information Systems Engineering and Management, Vol. 10 No. 2s (2025)

Thompson, D., & White, S. (2024).Exploring the role of social media analytics in enhancing customer relationship management (CRM) strategies in retail banking.*Journal of Retail Banking and Analytics*, 42(3), 76-89.

Zebua W., (2025), the role of Digital Transformation in Accounting System for the Transparency and Accountability of MAME Financial Statements. University Pancasila, Indonesia. 5.