MRS Journal of Multidisciplinary Research and Studies
ISSN *(Online) 3049-1398*
Vol-3, Iss-9 (September-2026)
Journal homepage: https://mrspublisher.com/journals

Cybersecurity Challenges in Nigeria's Integrated Personnel and Payroll Information System (IPPIS: Implications for Public Sector Accountability (2020-2025)

Uyoosu Ronald Terfa[1*], Dr Victor Ude-Umanta PhD[2] & Nengean Tersugh[3]

[*1]Imo State University Owerri

[2]Department of Political Science Federal University Wukari

[3]Department of Banking and finance Federal University Wukari

Received: 22 / 07 / 2026	Accepted: 29 / 08 / 2026	Published: 13 / 09 / 2026

Abstract: The increasing adoption of digital technologies has transformed public administration by enhancing efficiency, transparency, and accountability. In Nigeria, the Integrated Personnel and Payroll Information System (IPPIS) was introduced to improve payroll administration, eliminate ghost workers, and strengthen public financial management. Despite these achievements, the growing dependence on digital platforms has exposed government information systems to cybersecurity threats capable of undermining accountability and public trust. This study examined the cybersecurity challenges confronting the IPPIS and their implications for public sector accountability. Specifically, the study investigated the effects of cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance on public sector accountability. A cross-sectional survey research design was adopted, and primary data were collected through structured questionnaires administered to employees of selected Ministries, Departments, and Agencies (MDAs) operating under the IPPIS framework. Data were analysed using descriptive statistics and multiple regression analysis with the Statistical Package for the Social Sciences (SPSS) Version 27. The findings revealed that cybersecurity control measures significantly enhance public sector accountability ($\beta = 0.470$, $p < .05$), while cybersecurity policy compliance exerts the strongest positive influence ($\beta = 0.586$, $p < .05$). Conversely, cybersecurity threats had a negative but statistically insignificant effect ($\beta = –0.068$, $p > .05$). The study concludes that effective cybersecurity governance is indispensable for sustaining transparency, accountability, and integrity in Nigeria's digital public administration. It recommends continuous investment in cybersecurity infrastructure, strict enforcement of cybersecurity policies, regular staff capacity building, and strengthened institutional governance to improve the resilience of government information systems.

Keywords: *Cybersecurity, IPPIS, Public Sector Accountability, Digital Governance, Cybersecurity Policy Compliance, Nigeria.*

Cite this article: Terfa, U. R., Ude-Umanta, V. & Tersugh, N. (2026). Cybersecurity Challenges in Nigeria's Integrated Personnel and Payroll Information System (IPPIS: Implications for Public Sector Accountability (2020-2025). *MRS Journal of Multidisciplinary Research and Studies, 3(9), 48-54.*

Introduction

Digital transformation has fundamentally reshaped public administration by enabling governments to automate administrative processes, improve service delivery, strengthen financial management, and promote institutional transparency. The adoption of Information and Communication Technology (ICT) has become a major strategy for improving governance, reducing operational inefficiencies, and enhancing accountability in both developed and developing countries (Organisation for Economic Co-operation and Development [OECD], 2024; World Bank, 2024).

In Nigeria, one of the most significant public sector digital reforms is the Integrated Personnel and Payroll Information System (IPPIS), introduced by the Federal Government to centralize payroll administration and eliminate persistent payroll irregularities. Prior to the implementation of IPPIS, the public service experienced widespread payroll fraud, including ghost workers, duplicate salary payments, inaccurate personnel records, and weak expenditure control. Through the integration of personnel and payroll information into a unified electronic platform, IPPIS has significantly improved payroll transparency, strengthened financial accountability, and enhanced the management of public resources (Agbata & Oranefo, 2022; Office of the Accountant-General of the Federation [OAGF], 2024).

Despite these achievements, the increasing dependence on digital technologies has introduced significant cybersecurity risks. Government information systems have become attractive targets for cybercriminals seeking unauthorized access to confidential personnel and financial information. Cyber threats such as phishing attacks, ransomware, malware, insider abuse, identity theft, and unauthorized system access threaten the confidentiality, integrity, and availability of critical government databases. Consequently, cybersecurity has become a strategic governance issue rather than merely a technical concern (National Institute of Standards and Technology [NIST], 2024).

Cybersecurity governance encompasses the policies, technologies, institutional frameworks, and organizational practices designed to safeguard digital assets from evolving cyber

Copyright © 2026 The Author(s): This open-access article is distributed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0), permitting non-commercial use, sharing, and reproduction with proper credit to the author(s) and source.

threats. Effective cybersecurity governance ensures the confidentiality, integrity, and availability of information while protecting public institutions from financial losses, operational disruptions, and reputational damage (International Organization for Standardization [ISO], 2022; NIST, 2024).

Although Nigeria has strengthened its legal and regulatory frameworks through initiatives such as the Cybercrimes (Prohibition, Prevention, etc.) Act, the Nigeria Data Protection Act, and the National Cybersecurity Framework, many public institutions continue to experience inadequate technological infrastructure, insufficient cybersecurity funding, limited institutional capacity, shortages of skilled cybersecurity professionals, and low cybersecurity awareness among employees (National Information Technology Development Agency [NITDA], 2024; National Bureau of Statistics [NBS], 2024). These institutional deficiencies increase the vulnerability of critical government platforms, including the IPPIS.

Cybersecurity vulnerabilities within the IPPIS have implications beyond technological disruptions. Unauthorized manipulation of payroll databases, data breaches, identity theft, and cyber-enabled financial fraud can weaken transparency, undermine accountability, compromise public confidence, and reduce the effectiveness of digital governance reforms. Consequently, strengthening cybersecurity has become essential for protecting public resources and ensuring sustainable public sector accountability (OECD, 2024; World Bank, 2024).

Previous empirical studies have demonstrated that IPPIS has significantly reduced payroll fraud and improved accountability within Nigeria's public service (Agbata & Oranefo, 2022; Danbala et al., 2024). Similarly, cybersecurity research has examined organizational security practices, employee cybersecurity behaviour, and policy compliance across different sectors (Nguyen et al., 2024; Okigui et al., 2024). However, limited empirical evidence exists regarding the combined influence of cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance on public sector accountability within Nigeria's IPPIS environment. Addressing this gap is essential for strengthening cybersecurity governance and sustaining digital public sector reforms.

Accordingly, this study investigates the cybersecurity challenges confronting Nigeria's Integrated Personnel and Payroll Information System (IPPIS) and examines their implications for public sector accountability. Specifically, it evaluates how cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance influence accountability within the Nigerian public service. The findings contribute to the growing literature on digital governance, cybersecurity, and public financial management while providing practical recommendations for strengthening the security and accountability of government information systems.

Objectives of the study

The general objective of this study is to examine the cybersecurity challenges confronting Nigeria's Integrated Personnel and Payroll Information System (IPPIS) and their implications for public sector accountability.

Specifically, the study seeks to:

i. Examine the effect of cybersecurity threats on public sector accountability within the IPPIS.
ii. Determine the effect of cybersecurity control measures on public sector accountability.
iii. Assess the influence of cybersecurity policy compliance on public sector accountability.
iv. Evaluate the combined effect of cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance on public sector accountability.

Research Questions

The following research questions were formulated to guide the study:

i. What effect do cybersecurity threats have on public sector accountability in Nigeria's Integrated Personnel and Payroll Information System (IPPIS)?
ii. How do cybersecurity control measures influence public sector accountability in Nigeria's Integrated Personnel and Payroll Information System (IPPIS)?
iii. To what extent does cybersecurity policy compliance influence public sector accountability in Nigeria's Integrated Personnel and Payroll Information System (IPPIS)?
iv. What is the combined effect of cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance on public sector accountability within the IPPIS framework?

Research Hypotheses

The following null hypotheses guided the study:

i. H_{01}: Cybersecurity threats have no statistically significant effect on public sector accountability within the IPPIS.
ii. H_{02}: Cybersecurity control measures have no statistically significant effect on public sector accountability within the IPPIS.
iii. H_{03}: Cybersecurity policy compliance has no statistically significant effect on public sector accountability within the IPPIS.
iv. H_{04}: Cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance have no statistically significant joint effect on public sector accountability within the IPPIS.

Conceptual Review

Public Sector Accountability

Public sector accountability refers to the obligation of government institutions and public officials to explain, justify, and accept responsibility for their actions, decisions, and the management of public resources. It is a fundamental principle of good governance that promotes transparency, integrity, responsiveness, and efficient service delivery. Accountability requires public institutions to operate within established legal and ethical frameworks while ensuring that public funds are utilized effectively and in the public interest (Organisation for Economic Co-operation and Development [OECD], 2024). With the increasing adoption of digital governance, accountability extends beyond financial reporting to include the protection of government information systems and digital assets. Public institutions must therefore guarantee the confidentiality, integrity, and availability of information stored on electronic platforms. Consequently, effective cybersecurity governance has become an essential component of

public sector accountability because weaknesses in information security can undermine transparency, public confidence, and institutional credibility (World Bank, 2024).

Cybersecurity Challenges

Cybersecurity challenges refer to the various threats, vulnerabilities, and risks capable of compromising the security of information systems and digital infrastructure. These challenges arise from technological weaknesses, human error, insider abuse, and external cyberattacks. Common cybersecurity challenges include phishing, malware, ransomware, unauthorized access, identity theft, insider threats, and data breaches (National Institute of Standards and Technology [NIST], 2024).

Within the public sector, cybersecurity challenges have become increasingly significant because government agencies manage large volumes of confidential personnel, financial, and administrative information. Failure to address these challenges can disrupt public service delivery, expose sensitive information, and weaken accountability in government institutions (National Information Technology Development Agency [NITDA], 2024).

Cybersecurity Threats

Cybersecurity threats are malicious activities that exploit weaknesses in information systems to gain unauthorized access, manipulate data, or disrupt organizational operations. These threats may originate from cybercriminals, hackers, organized criminal groups, or malicious insiders. Common examples include phishing attacks, ransomware, malware infections, denial-of-service attacks, identity theft, and unauthorized system access (NIST, 2024). For government information systems such as the Integrated Personnel and Payroll Information System (IPPIS), cybersecurity threats pose serious risks because unauthorized access to payroll databases may lead to payroll fraud, financial losses, disruption of government operations, and erosion of public trust.

Cybersecurity Control Measures

Cybersecurity control measures are the administrative, technical, and physical safeguards implemented to protect digital systems against cyber threats. These measures include encryption technologies, multi-factor authentication, firewalls, intrusion detection systems, access control mechanisms, vulnerability assessments, regular software updates, security monitoring, incident response plans, and routine data backup (International Organization for Standardization [ISO], 2022; NIST, 2024). Organizations with effective cybersecurity controls are better able to prevent cyberattacks, maintain data integrity, ensure business continuity, and strengthen public confidence in digital governance.

Cybersecurity Policy Compliance

Cybersecurity policy compliance refers to adherence to established cybersecurity laws, regulations, standards, and organizational policies governing the protection of information assets. Compliance requires employees to observe security procedures relating to password management, user authentication, access control, software updates, data protection, and incident reporting (ISO, 2022). Within the Nigerian public sector, compliance with cybersecurity policies enhances organizational resilience, reduces security vulnerabilities, and strengthens accountability by ensuring that sensitive government information is adequately protected (NITDA, 2024).

Integrated Personnel and Payroll Information System (IPPIS)

The Integrated Personnel and Payroll Information System (IPPIS) is an electronic human resource and payroll management platform established by the Federal Government of Nigeria to improve transparency and accountability in payroll administration. The system centralizes personnel records, automates salary payments, eliminates ghost workers, and strengthens expenditure control across Ministries, Departments, and Agencies (MDAs) (Office of the Accountant-General of the Federation [OAGF], 2024). Although IPPIS has significantly improved payroll administration, its effectiveness depends largely on the security of its information infrastructure. Protecting the confidentiality and integrity of payroll data therefore remains essential for sustaining public sector accountability.

Theoretical Framework

This study is anchored on Routine Activity Theory (RAT) developed by Cohen and Felson (1979). The theory posits that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. Although originally developed to explain conventional crimes, the theory has become widely applicable in cybersecurity research because cybercrime follows similar behavioural patterns (Cohen & Felson, 1979).

Within the context of the IPPIS, cybercriminals represent motivated offenders, while the payroll database constitutes a suitable target because it contains valuable personnel and financial information. Weak cybersecurity infrastructure, poor employee awareness, inadequate monitoring, and non-compliance with security policies create opportunities for successful cyberattacks. Conversely, robust cybersecurity controls—including multi-factor authentication, encryption, intrusion detection systems, continuous monitoring, employee awareness programmes, and strict policy compliance—serve as capable guardians that reduce cyber risks (NIST, 2024; NITDA, 2024).

Routine Activity Theory therefore provides a suitable framework for explaining how cybersecurity governance influences accountability within Nigeria's public sector. Effective cybersecurity controls reduce opportunities for cybercrime, strengthen information security, and improve transparency, accountability, and institutional resilience.

Empirical Review

Empirical evidence demonstrates that cybersecurity governance significantly influences the effectiveness of digital public administration.

Ilawagbon and Ajisebiyawo (2024) investigated electronic administration and public sector accountability in Nigeria using a qualitative research design. Their findings revealed that digital platforms such as IPPIS, GIFMIS, and the Open Treasury Portal significantly improved transparency, accountability, and payroll administration. However, inadequate ICT infrastructure, cybersecurity concerns, and insufficient staff training limited the effectiveness of these digital reforms.

Nguyen et al. (2024) examined cybersecurity behaviour among public sector employees in Vietnam using a cross-sectional survey design. The study found that phishing attacks, insider threats, poor cybersecurity awareness, and unsafe online practices significantly increased organizational vulnerability. The authors

recommended continuous cybersecurity awareness programmes and stronger organizational security policies.

Woods and Seymour (2024) conducted a meta-review of cybersecurity intervention studies and concluded that multi-factor authentication, software patch management, cloud email protection, vulnerability assessments, and continuous security monitoring are among the most effective cybersecurity controls for reducing cyber risks.

Okigui et al. (2024) investigated cybersecurity policy compliance using a qualitative case-study approach. Their findings indicated that weak enforcement mechanisms, policy complexity, employee resistance, and insider threats significantly reduced compliance with cybersecurity policies. They emphasized regular awareness programmes and stronger institutional enforcement to improve organizational information security.

Danbala et al. (2024) examined the effectiveness of IPPIS in Nigeria and reported that the system significantly reduced payroll fraud, eliminated ghost workers, and improved accountability in payroll administration. Nevertheless, cybersecurity vulnerabilities, technical failures, and inadequate ICT infrastructure remained major constraints affecting the sustainability of the system.

Critique of Previous Studies

Although previous studies have contributed significantly to knowledge on digital governance and cybersecurity, several methodological and contextual limitations remain. Many studies relied on qualitative research designs, limiting the statistical generalization of their findings (Ilawagbon & Ajisebiyawo, 2024; Okigui et al., 2024). Others were conducted in foreign institutional settings with different legal and technological environments, making their findings less applicable to Nigeria (Nguyen et al., 2024).

Similarly, studies focusing on IPPIS concentrated mainly on payroll efficiency and the elimination of ghost workers while paying limited attention to cybersecurity governance (Danbala et al., 2024). Few studies have simultaneously examined cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance as predictors of public sector accountability within the Nigerian public service.

This study addresses these limitations by employing a quantitative research design to examine both the individual and combined effects of these cybersecurity dimensions on public sector accountability within the IPPIS. The findings provide empirical evidence capable of informing cybersecurity policy, strengthening digital governance, and improving accountability in Nigeria's public financial management system.

Methodology

This study adopted a cross-sectional survey research design to examine the influence of cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance on public sector accountability within Nigeria's Integrated Personnel and Payroll Information System (IPPIS). The design was considered appropriate because it enabled the collection of quantitative data from respondents at a single point in time and facilitated the examination of relationships among the study variables (Creswell & Creswell, 2023).

Results

Model Summary

Table 1: Model Summary

S/N	MODEL	R	R^2	ADJUSTED R^2	STD. ERROR	F
1.	1	0.997	0.995	0.994	0.306	17014.011

Source: Field Survey Analysis using SPSS Version 27 (2026).

Table 1 presents the model summary for the regression analysis. The correlation coefficient (R = 0.997) indicates a very strong positive relationship between the explanatory variables and public sector accountability. The coefficient of determination (R^2 = 0.995) implies that approximately 99.5% of the variation in public sector accountability is explained jointly by cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance. The adjusted R^2 of 0.994 further confirms the robustness of the model after adjusting for the number of predictors.

Analysis of Variance (ANOVA)

Table 2: ANOVA Results

S/N	Source	Sum of Squares	Df	Mean Square	F	Sig
1.	Regression	4785.954	3	1595.318	17014.11	.000
2.	Residual	26.348	281	0.094		
3.	Total	4812.302	284			

Dependent Variable: Public Sector Accountability (PSA)

Source: Field Survey Analysis using SPSS Version 27 (2026).

The ANOVA results indicate that the regression model is statistically significant (F = 17014.011, p < .001). Therefore, the null hypothesis that cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance have no joint effect on public sector accountability is

rejected. This finding confirms that the explanatory variables collectively exert a significant influence on accountability within the IPPIS framework.

Regression Analysis

Table 3: Regression Coefficients

S/N	Variables	B	Std. Error	Beta	T	Sig	Decision
1.	Constant	0.119	0.037	-	3.219	.001	Significant
2.	Cybersecurity control measures (CCM)	0.470	0.040	0.467	11.712	.000	Supported
3.	Cybersecurity Policy compliance (CPC)	0.586	0.084	0.602	6.967	.000	Supported
4.	Cybersecurity Threats (CST)	-0.068	0.067	-0.070	-1.007	.315	Not supported

Dependent Variable: Public Sector Accountability (PSA)

Source: Field Survey Analysis using SPSS Version 27 (2026).

The regression analysis indicates that cybersecurity control measures exert a positive and statistically significant influence on public sector accountability ($\beta = 0.470$, $p < .001$). This finding suggests that strengthening cybersecurity safeguards, including access controls, encryption, intrusion detection systems, and continuous monitoring, enhances transparency and accountability within the IPPIS.

Similarly, cybersecurity policy compliance has a positive and statistically significant effect on public sector accountability ($\beta = 0.586$, $p < .001$). Among all explanatory variables, policy compliance emerged as the strongest predictor, indicating that strict adherence to cybersecurity policies substantially improves accountability in digital public administration.

Conversely, cybersecurity threats exhibited a negative coefficient ($\beta = –0.068$) but were not statistically significant ($p = .315$). This finding suggests that although cyber threats have the potential to undermine accountability, their impact is considerably reduced where effective cybersecurity controls and policy compliance mechanisms are adequately implemented.

Summary of Hypotheses Testing

Table 4: Decision on Research Hypotheses

S/N	Hypothesis	Decision
1.	H_{01}: Cybersecurity threats have no significant effect on public sector accountability.	Accepted
2.	H_{02}: Cybersecurity control measures have no significant effect on public sector accountability.	Rejected
3.	H_{03}: Cybersecurity policy compliance has no significant effect on public sector accountability.	Rejected
4.	H_{04}: Cybersecurity threats, cybersecurity control measures, and cybersecurity policy compliance have no joint significant effect on public sector accountability.	Rejected

The findings demonstrate that cybersecurity governance plays a significant role in enhancing public sector accountability. While cybersecurity threats alone did not significantly influence accountability, effective cybersecurity control measures and strict policy compliance were found to be critical determinants of accountability within Nigeria's IPPIS.

Discussion of Findings

The findings of this study demonstrate that cybersecurity governance is a critical determinant of public sector accountability within Nigeria's Integrated Personnel and Payroll Information System (IPPIS). The regression analysis showed that cybersecurity control measures and cybersecurity policy compliance significantly improve accountability, whereas cybersecurity threats exhibited a negative but statistically insignificant effect. These findings reinforce the growing consensus that effective cybersecurity governance is essential for sustaining transparency, integrity, and efficiency in digital public administration.

The study established that cybersecurity control measures have a positive and statistically significant influence on public sector accountability. This finding implies that implementing robust security mechanisms such as encryption, multi-factor authentication, intrusion detection systems, access controls, continuous monitoring, and regular vulnerability assessments significantly enhances the integrity and reliability of payroll administration. Strong cybersecurity controls reduce opportunities for unauthorized access, payroll manipulation, and cyber-enabled fraud, thereby strengthening accountability in the management of public resources. This finding corroborates the study of Woods and Seymour (2024), who identified proactive cybersecurity controls as fundamental to reducing cyber risks and improving organizational resilience. It also supports the findings of Danbala et al. (2024),

who reported that strengthening ICT infrastructure and cybersecurity significantly improves the effectiveness of IPPIS in Nigeria.

The findings further revealed that cybersecurity policy compliance is the strongest predictor of public sector accountability. This suggests that strict adherence to cybersecurity policies, data protection regulations, and organizational information security standards enhances transparency by protecting the confidentiality, integrity, and availability of government information. Effective compliance also strengthens internal control systems and reduces institutional vulnerabilities. This result is consistent with the findings of Okigui et al. (2024), who emphasized that effective implementation and enforcement of cybersecurity policies significantly improve organizational information security. Similarly, the ISO/IEC 27001:2022 standard recognizes policy compliance as a critical requirement for effective information security management (International Organization for Standardization [ISO], 2022).

Although cybersecurity threats exhibited a negative relationship with public sector accountability, the effect was not statistically significant. This finding suggests that the mere existence of cyber threats does not necessarily undermine accountability where effective cybersecurity controls and policy compliance mechanisms are already institutionalized. Organizations with mature cybersecurity governance frameworks are better equipped to detect, prevent, and respond to cyber incidents before they significantly affect organizational performance. This finding aligns with Bada and Nurse (2022), who argued that the impact of cyber threats depends largely on organizational preparedness, resilience, and security governance rather than the frequency of threats themselves. The findings strongly support Routine Activity Theory (Cohen & Felson, 1979), which posits that crime becomes less likely when capable guardians exist. Within the IPPIS environment, cybersecurity controls and policy compliance function as capable guardians by reducing opportunities for cybercrime and protecting sensitive payroll information. Consequently, strengthening cybersecurity governance promotes transparency, safeguards public resources, and enhances accountability in Nigeria's digital public administration.

Conclusion

This study examined the cybersecurity challenges confronting Nigeria's Integrated Personnel and Payroll Information System (IPPIS) and their implications for public sector accountability. The findings revealed that effective cybersecurity governance is fundamental to improving accountability, transparency, and efficiency in public financial management. Cybersecurity controls and policy compliance significantly enhance information integrity, internal controls, and payroll security, with policy compliance emerging as the strongest determinant of accountability. Although cybersecurity threats negatively influence accountability, their impact is not significant where effective cybersecurity governance is in place. The study therefore concludes that sustained investment in cybersecurity infrastructure, robust security controls, policy compliance, and employee capacity development is essential for strengthening the resilience and sustainability of the IPPIS.

Recommendations

- Strengthen cybersecurity infrastructure: The Federal Government should invest in modern cybersecurity technologies, including multi-factor authentication, encryption, intrusion detection systems, continuous monitoring tools, and vulnerability assessment mechanisms to enhance the security of the IPPIS.
- Improve cybersecurity policy compliance: Ministries, Departments, and Agencies (MDAs) should institutionalize regular compliance audits and enforce adherence to the Nigeria Data Protection Act, the National Cybersecurity Framework, and organizational information security policies.
- Promote continuous capacity building: Government should organize regular cybersecurity awareness programmes, workshops, and professional training for IPPIS users, ICT personnel, payroll administrators, and other public sector employees to reduce human-related cybersecurity risks.

Contribution to Knowledge

This study contributes to the growing literature on cybersecurity and digital governance in several important ways. It provides empirical evidence on the relationship between cybersecurity threats, cybersecurity control measures, cybersecurity policy compliance, and public sector accountability within Nigeria's Integrated Personnel and Payroll Information System (IPPIS). Unlike previous studies that focused primarily on banking or private-sector cybersecurity, this research specifically addresses cybersecurity governance in Nigeria's public sector. the study also establishes that cybersecurity policy compliance and cybersecurity control measures are significant determinants of public sector accountability, thereby highlighting the importance of institutional cybersecurity governance in strengthening digital public administration.

Limitations of the Study

The study was limited to selected Federal Ministries, Departments, and Agencies operating under the IPPIS, thereby limiting the generalizability of the findings to all public institutions in Nigeria. The study also relied primarily on questionnaire responses, making the findings dependent on respondents' perceptions and susceptible to response bias. Furthermore, limited access to confidential cybersecurity information relating to the technical architecture and operational security of the IPPIS restricted the examination of some advanced cybersecurity issues.

Suggestions for Further Research

Future studies should investigate additional cybersecurity variables such as cybersecurity awareness, digital literacy, organizational security culture, incident response capability, and cyber resilience to provide a broader understanding of accountability within digital public administration. Comparative studies involving other government digital platforms such as the Government Integrated Financial Management Information System (GIFMIS) and the Treasury Single Account (TSA) are also recommended. In addition, longitudinal and mixed-methods studies would provide deeper insights into the long-term effects of cybersecurity governance on public sector accountability.

References

1. Agbata, O. C., & Oranefo, P. C. (2022). Integrated Personnel and Payroll Information System (IPPIS) and public sector accountability in Nigeria. Journal of Public Administration and Governance, 12(3), 45–60.
2. Bada, M., & Nurse, J. R. C. (2022). The social and human factors of cybersecurity: A systematic review. Computers & Security, 114, 102609. https://doi.org/10.1016/j.cose.2021.102609
3. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589
4. Creswell, J. W., & Creswell, J. D. (2023). Research design: Qualitative, quantitative, and mixed methods approaches (6th ed.). Sage.
5. Danbala, A., Suleiman, M., & Bala, A. (2024). Integrated Personnel and Payroll Information System (IPPIS) and payroll accountability in Nigeria's public service. African Journal of Public Administration and Management, 9(1), 33–49.
6. Ilawagbon, T. O., & Ajisebiyawo, A. A. (2024). E-administration and public sector accountability in Nigeria. International Journal of Public Administration and Digital Governance, 11(2), 85–101.
7. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements. https://www.iso.org
8. Kothari, C. R. (2019). Research methodology: Methods and techniques (4th ed.). New Age International Publishers.
9. National Bureau of Statistics. (2024). Nigeria ICT sector report. National Bureau of Statistics.
10. National Information Technology Development Agency. (2024). National cybersecurity framework and strategy. https://nitda.gov.ng
11. National Institute of Standards and Technology. (2024). Cybersecurity framework (CSF 2.0). U.S. Department of Commerce. https://www.nist.gov/cyberframework
12. Nguyen, T. H., Tran, P. V., & Le, M. Q. (2024). Factors influencing cybersecurity behaviour among public sector employees in Vietnam. Government Information Quarterly, 41(2), 101912.
13. Office of the Accountant-General of the Federation. (2024). Integrated Personnel and Payroll Information System (IPPIS). Federal Government of Nigeria. https://oagf.gov.ng
14. Okigui, C., Cronjé, J., & Francke, E. (2024). Cybersecurity policy compliance in organizations: An actor-network theory perspective. Information & Computer Security, 32(1), 73–91.
15. Organisation for Economic Co-operation and Development. (2024). Government at a glance 2024. OECD Publishing.
16. World Bank. (2024). Digital development and governance report. World Bank.