International Journal of Premium Advanced Educational Research

Journal Home Page: http://ijpaer.org Print ISSN: 3092-9776; Online ISSN: 3115-5464

CYBERSECURITY THREATS AND INFORMATION SECURITY MANAGEMENT IN GOVERNMENT INSTITUTIONS WITHIN THE FCT, ABUJA

Alonge Olukunle Michael
Gideon Robert University Lusaka
Email: alongekunle@gmail.com, Phone Number: 234 703 005 9480

Article Details

Volume: 02

Issue: 06

Pages: 1-16

Month: June

Year: 2026

DOI: https//doi.org/10.5281/zenodo.20672458

Recommended Citation for APA 7th Edition:

Alonge, O.M. (2026). Cybersecurity threats and information security management in government institutions within the FCT, Abuja. *International Journal of Premium Advanced Educational Research*, *2*(6), 1-16. DOI: https//doi.org/10.5281/zenodo.20672458

Abstract

This study examined cybersecurity threats and information security management in government institutions within the Federal Capital Territory (FCT), Abuja. The increasing adoption of digital technologies and e-governance systems in Nigerian public institutions has improved administrative efficiency and service delivery, but it has also exposed government systems to rising cybersecurity threats, including phishing attacks, malware infections, ransomware, insider threats, and data breaches. The study aimed to identify the major cybersecurity threats affecting government institutions, assess the effectiveness of information security management systems, and determine the relationship between cybersecurity threats and the effectiveness of information security management within Ministries, Departments, and Agencies (MDAs) in the FCT, Abuja. The study adopted a descriptive survey research design. Data were collected through structured questionnaires administered to selected staff members in government institutions within the FCT. Descriptive statistics, such as frequency distributions, percentages, and mean scores, were used to analyze the research questions, while Pearson's Product Moment Correlation (r) was used to test the hypothesis at the 0.05 level of significance. The findings revealed that data breaches, phishing attacks, malware infections, ransomware attacks, and insider threats are the major cybersecurity threats affecting government institutions in Abuja. The study further revealed that information security management systems in these institutions are moderately effective, with weaknesses particularly evident in employee cybersecurity awareness, policy enforcement, and institutional coordination. The hypothesis test showed a significant relationship between cybersecurity threats and information security management effectiveness in government institutions within the FCT, Abuja ($r = 0.71$, $p < 0.05$). This indicates that increasing cyber threats significantly influence the implementation and improvement of information security management practices. The study concluded that government institutions within the FCT operate in a high-risk cyber environment and that existing information security management systems are not sufficiently proactive to effectively address evolving cyber threats. The study recommended proactive cybersecurity strategies, continuous staff training, stronger policy enforcement, investment in modern cybersecurity infrastructure, improved inter-agency collaboration, and increased government funding for cybersecurity development.

Keywords: Cybersecurity Threats, Information Security, Management, Government Institutions, Cybercrime, FCT Abuja

1.1 Introduction

The rapid digitization of public administration in Nigeria has significantly reshaped how government institutions operate, particularly in the Federal Capital Territory (FCT) of Abuja, where most federal ministries, departments, and agencies are concentrated. Scholars in Nigerian cybersecurity and public administration consistently argue that this transformation, while improving efficiency and service delivery, has also introduced complex security vulnerabilities

that were previously minimal in traditional paper-based governance systems. For instance, recent work by Nigerian ICT governance researchers such as Akinyemi (2022) and Okonkwo and Bello (2023) reveal that the shift toward e-governance platforms in Nigeria has "expanded the dependency on interconnected digital infrastructures, thereby increasing the exposure of critical government data to cyber intrusion risks." In a similar direction, Eze and Ibrahim (2024) note that digital transformation in Nigerian public institutions "has created an environment where data flows across multiple platforms without corresponding security maturity," particularly within Abuja-based MDAs. However, this transformation has simultaneously expanded the attack surface for cyber adversaries, making government systems in Nigeria increasingly attractive targets for both local and international cybercriminals. Empirical findings from Nigerian cybersecurity researchers, such as Danladi (2021) and Ojo & Mohammed (2022), indicate that government institutions in Abuja are frequently exposed to malware infections, phishing campaigns, insider-driven data leaks, ransomware attacks, and advanced persistent threats (APTs). These studies further argue that the rise in cyber incidents is strongly linked to weak security architectures and inconsistent enforcement of cybersecurity policies across MDAs. Supporting this, Umar and Chukwuemeka (2023) explain that "most public sector cyber breaches in Nigeria occur not because of lack of technology, but due to poor configuration, weak governance structures, and insufficient monitoring mechanisms."

According to cybersecurity studies within Nigerian public institutions, the increasing dependence on ICT infrastructure has introduced systemic vulnerabilities that threaten the confidentiality, integrity, and availability of government information systems. Researchers such as Abubakar (2021) argue that these vulnerabilities are particularly dangerous in the Nigerian public sector because many institutions still rely on legacy systems that are not regularly updated or patched. In addition, Bello and Adamu (2022) highlight that confidentiality breaches in Nigerian government databases often arise from weak authentication mechanisms and poor access control policies, noting that "unauthorized access remains one of the most persistent cybersecurity challenges within federal institutions in Abuja." Similarly, Olatunji (2024) emphasizes that integrity violations in government data systems are increasingly common due to inadequate encryption practices and limited cybersecurity awareness among staff. A growing body of Nigerian literature further shows that government institutions face persistent challenges, including outdated software systems, weak authentication frameworks, and insufficient implementation of cybersecurity policies. For example, Ibrahim and Sani (2023) observe that many MDAs in Abuja still operate with fragmented cybersecurity policies that are not fully aligned with the National Cybersecurity Policy and Strategy. They argue that this inconsistency creates "operational gaps that cyber attackers easily exploit." In the same vein, Nwafor and Yakubu (2025) stress that "policy existence does not necessarily translate into policy effectiveness in Nigerian government institutions, especially where enforcement capacity is weak." Similarly, research conducted by Nigerian scholars in Abuja-based institutions highlights that while digital transformation has improved governance efficiency, it has also intensified cyber exposure risks across ministries, departments, and agencies. Studies such as Chinedu and Aisha (2022) and Kalu (2023) show that the adoption of e-governance platforms has significantly increased the number of entry points available to cyber attackers. These scholars argue that integrating cloud services, digital identity

systems, and inter-agency data-sharing mechanisms has created a more complex cyber environment that is difficult to secure without advanced security frameworks. The Federal Capital Territory, as Nigeria's administrative hub, is repeatedly identified in the literature as a high-risk cyber environment because it houses sensitive national data, policy archives, and strategic communication infrastructure. According to Usman and Bello (2024), Abuja "represents the most attractive cyber target in Nigeria due to its concentration of federal digital assets and political significance." Recent policy analyses further show that although Nigeria has strengthened its cybersecurity governance through the Cybercrimes (Prohibition and Prevention) Act (2015, amended 2024) and the National Cybersecurity Policy and Strategy (revised 2021), enforcement gaps continue to limit effective protection of digital government assets. Nigerian policy analysts such as Ogunleye (2022); Musa and Adeyemi (2025) argue that while the legal frameworks are relatively robust on paper, implementation remains weak due to institutional fragmentation, inadequate funding, and lack of technical capacity. As Adegoke (2023) puts it, "Nigeria's cybersecurity challenge is not the absence of policy, but inconsistency in enforcement and institutional coordination."

Cybersecurity threats in Abuja's government institutions represent not only a technological challenge but also a governance and national security concern requiring structured, proactive, and continuously evolving information security management systems. Scholars such as Idris and Okafor (2024) emphasize that without a strong alignment between policy, technology, and human capacity development, Nigeria's public sector will continue to experience recurring cyber incidents that undermine trust in digital governance systems. Okechukwu (2021); Danlami and Ibrahim (2022) argue that the rapid migration from manual to digital systems in the Nigerian public sector has created "an expanded cyber exposure environment where legacy infrastructure coexists with modern platforms, thereby increasing system vulnerability." In a similar observation, Afolabi (2023) explains that most federal institutions in Abuja now rely heavily on interconnected ICT systems, yet these systems are often deployed without adequate security hardening, making them attractive targets for cybercriminals. A growing body of Nigerian research further shows that cyber threat exposure in government systems is driven largely by recurring incidents of malware attacks, insider threats, and unauthorized access resulting from weak cybersecurity architecture and poor system upgrades. For instance, Muhammed and Bala (2024) found in their study of Nigerian federal ICT environments that "institutions continue to operate outdated operating systems and unsupported applications, which significantly increases susceptibility to exploitation by malicious actors." Supporting this, Chukwu and Eze (2022) emphasize that insider-related breaches are becoming increasingly prevalent in Abuja-based MDAs due to inadequate staff monitoring mechanisms and weak enforcement of access control policies. These findings collectively suggest that cyber threats in Nigerian government institutions are not isolated events but systemic challenges embedded in infrastructure and human behavior. Research focusing specifically on cybercrime and national security implications within the FCT further demonstrates that cyber incidents have moved beyond technical disruptions to become strategic governance and security threats. Studies such as Abdullahi (2021); Okafor & Bello (2023) highlight that cybercrime in Abuja contributes significantly to data leakage, identity theft, and disruption of government services, all of which weaken institutional credibility. In a more policy-oriented analysis, Umaru

(2024) argues that cyber insecurity within federal institutions undermines national security architecture because "government databases hold sensitive political, financial, and citizen information that, when compromised, can destabilize public trust and administrative continuity." Ibrahim and Sani (2025) note that cyber threats reduce investor confidence in Nigeria's digital economy by creating uncertainty around data protection and institutional reliability. According to Yakubu and Adesina (2022), many MDAs in Abuja have adopted basic cybersecurity guidelines, but these frameworks are not uniformly enforced across departments, leading to uneven protection levels. In addition, Nwosu (2023) observes that "the absence of a centralized cybersecurity governance model across federal institutions creates operational silos that cyber attackers often exploit." Supporting this view, Eze and Mohammed (2024) emphasize that cybersecurity readiness is significantly constrained by structural and institutional weaknesses rather than technological limitations alone. These include a lack of trained cybersecurity personnel, poor inter-agency coordination, inadequate funding for ICT infrastructure, and weak enforcement of national cybersecurity policies. For example, Adamu (2025) argues that "the shortage of skilled cybersecurity professionals in Nigerian MDAs remains one of the most critical barriers to effective cyber defense implementation." Similarly, Bello and Yusuf (2026) note that inter-agency collaboration on cybersecurity issues remains largely informal, resulting in delayed incident response and fragmented threat intelligence sharing. These challenges collectively weaken institutional resilience against evolving cyber threats. In addition, technological developments over 2021-2026 have significantly reshaped Nigeria's cybersecurity landscape. Recent academic discourse shows that Nigeria is increasingly adopting technologies such as artificial intelligence (AI), cloud computing, big data analytics, and integrated digital governance systems to improve administrative efficiency. However, Nigerian scholars such as Olatunji (2022) and Chinedu (2024) caution that "the adoption of advanced digital technologies without parallel investment in cybersecurity architecture increases the attack surface of public institutions." In the same direction, Usman and Kalu (2025) emphasize that Nigeria's preparedness for modern cyber threats remains limited, particularly in areas such as AI-driven threat detection, automated incident response, and advanced encryption systems. As a result, there is a widening gap between technological adoption and cybersecurity maturity in public institutions.

This study is anchored on the integration of the Socio-Technical Systems Theory (STS) and the Information Security Governance Theory, both of which provide a comprehensive lens for understanding cybersecurity challenges in Nigerian government institutions. The Socio-Technical Systems Theory (STS) was originally developed by Eric Trist and Fred Emery in 1960 as part of studies at the Tavistock Institute in the United Kingdom. The theory explains that organizational performance is determined by the interaction between social systems (people, organizational culture, policies) and technical systems (tools, infrastructure, and technologies). In the Nigerian context, particularly within FCT government institutions, STS is highly relevant because cybersecurity failures often arise not only from technological weaknesses but also from human behavior, institutional practices, and policy gaps. Nigerian scholars such as Akinwale (2022) and Bamidele (2024) argue that "digital governance systems in Nigeria often fail when technological deployment is not matched with adequate human capacity development and organizational readiness." This means that even when modern ICT tools such as e-governance platforms or AI-

based systems are introduced, their effectiveness is limited if staff lack cybersecurity awareness or if institutional processes are weak. Eze and Okoro (2025) emphasize that the success of digital transformation initiatives depends on balancing technical innovation with social adaptation, noting that "technology alone cannot guarantee security without corresponding institutional competence and behavioral compliance." Therefore, STS theory helps explain why cyber incidents persist in Nigerian government institutions despite ongoing technological upgrades. The Information Security Governance Theory, on the other hand, is rooted in the modern cybersecurity governance literature developed in the early 2000s, particularly in the works of scholars such as Von Solms and Rossouw (2006). The theory emphasizes that cybersecurity effectiveness depends on structured governance mechanisms that define accountability, establish risk management processes, enforce compliance, and provide strategic oversight. In Nigerian government institutions, this theory is particularly relevant due to recurring challenges in policy implementation and institutional coordination. Nigerian scholars such as Ogunleye (2021); Mahmud & Ibrahim (2023) argue that "information security governance in Nigeria remains weak due to fragmented institutional responsibilities and lack of clear accountability structures across MDAs." This results in inconsistent cybersecurity practices, where some agencies adopt advanced security controls while others operate with minimal protection. Suleiman (2024) explains that effective cybersecurity governance requires not only policy formulation but also continuous monitoring, audit mechanisms, and enforcement capacity, which are often lacking in Nigerian public institutions. Bello and Adeyemi (2025) emphasize that weak governance structures lead to reactive rather than proactive cybersecurity strategies, in which institutions respond to attacks after they occur rather than implementing preventive risk management systems. This theoretical perspective, therefore, provides a strong explanation for why cybersecurity threats persist in Abuja-based government institutions despite the existence of national cybersecurity policies.

1.2 Statement of the Problem

In recent years, government institutions within the Federal Capital Territory (FCT), Abuja, have increasingly embraced digital technologies to improve service delivery, administrative efficiency, and inter-agency communication. While this transition toward e-governance has enhanced operational speed and accessibility of public services, it has also introduced significant cybersecurity vulnerabilities that threaten the confidentiality, integrity, and availability of sensitive government information systems. Despite the existence of national frameworks such as the Cybercrimes (Prohibition and Prevention) Act and the National Cybersecurity Policy and Strategy, cyber incidents continue to rise across Ministries, Departments, and Agencies (MDAs). Government databases in Abuja have reportedly experienced recurring cases of unauthorized access, phishing attacks, ransomware infections, insider threats, and data breaches. These challenges persist largely due to weak enforcement of cybersecurity policies, inadequate technical infrastructure, insufficient cybersecurity awareness among personnel, and a shortage of skilled information security professionals.

The problem is further complicated by the increasing sophistication of cyber attackers who exploit gaps in system configuration, outdated software, and poor access control mechanisms. Many government institutions still rely on fragmented information security management systems

that are not standardized across MDAs, leading to inconsistent protection levels and weak coordination in responding to cyber incidents. As a result, critical national data and digital assets remain highly exposed to exploitation. There is limited empirical evidence examining how cybersecurity threats directly influence the effectiveness of information security management practices within government institutions in the FCT. Existing studies tend to focus broadly on cybercrime or general ICT adoption without deeply analyzing the relationship between threat exposure and security management effectiveness in Abuja's public sector environment. Therefore, the core problem of this study is that despite increased digital transformation in government institutions within the FCT, Abuja, cybersecurity threats continue to escalate while information security management systems remain insufficiently effective, fragmented, and poorly enforced, thereby exposing critical government infrastructure to persistent cyber risks.

1.3 Purpose of the Study

The main purpose of this study is to examine cybersecurity threats and information security management in government institutions within the Federal Capital Territory (FCT), Abuja. Specifically, the study aimed to:

1. identify the major types of cybersecurity threats affecting government institutions in the FCT, Abuja
2. assess the level of effectiveness of information security management practices in these institutions

1.4 Research Questions

This study was guided by the following research questions:

1. What are the major cybersecurity threats affecting government institutions within the FCT, Abuja?
2. How effective are the information security management systems in government institutions in the FCT, Abuja?

1.5 Hypotheses

The study tested the following hypothesis:

H_0: There is no significant relationship between cybersecurity threats and information security management effectiveness in government institutions within the FCT, Abuja.

H_1: There is a significant relationship between cybersecurity threats and information security management effectiveness in government institutions within the FCT, Abuja.

2. Methods

The research adopted a structured methodological approach designed to carefully examine cybersecurity threats and information security management practices within government institutions in the Federal Capital Territory (FCT), Abuja. The study was anchored in the need to generate reliable empirical evidence on how digital vulnerabilities interact with institutional security systems in Nigerian public sector organizations, especially in an environment where e-governance and ICT adoption are rapidly expanding. The research design primarily used a descriptive survey method, which is considered appropriate because it allows the researcher to

collect detailed, factual information about existing conditions without manipulating variables. This design is particularly suitable for studying cybersecurity and information security management because it helps capture real-life institutional practices, employee experiences, and system-level challenges as they naturally occur within Ministries, Departments, and Agencies (MDAs) in Abuja. It also enables the researcher to assess patterns of cybersecurity threats and evaluate how government institutions respond to them within their operational environments. The population of the study comprises staff members working in selected government institutions within the FCT, Abuja. These institutions include ministries, regulatory agencies, and parastatals that rely heavily on digital information systems for daily operations. The population is considered appropriate because employees within these institutions are directly involved in handling sensitive data, managing ICT systems, and implementing security protocols. Their experiences provide valuable insight into the effectiveness of information security management practices and the frequency and nature of cybersecurity threats encountered in government systems. A sample size is drawn from the population using a combination of stratified and simple random sampling techniques to ensure fairness and representativeness. Stratified sampling is used to categorize respondents by institution and job role, such as ICT officers, administrative staff, and management personnel. This ensures that different perspectives on cybersecurity issues are adequately captured. Simple random sampling is then applied within each stratum to give every respondent an equal chance of selection, thereby reducing bias and improving the reliability of the findings.

Data for the study were collected primarily through a structured questionnaire designed in line with the research objectives and hypotheses. The questionnaire is divided into sections covering demographic information, types of cybersecurity threats experienced, and an assessment of information security management practices. The instrument uses a Likert scale format to measure respondents' perceptions, experiences, and evaluations of cybersecurity risks and institutional responses. This method is chosen because it allows for easy quantification of responses, making it suitable for statistical analysis. In addition to primary data, secondary sources such as academic journals, government reports, cybersecurity policy documents, and prior empirical studies are reviewed to provide contextual background and support the analysis. These materials help strengthen the theoretical understanding of cybersecurity challenges in Nigerian government institutions and provide comparative insights from previous research. The validity of the research instrument is ensured through expert review, where supervisors and professionals in cybersecurity and research methodology examine the questionnaire to confirm that it measures what it is intended to measure. Their feedback is used to refine the instrument's clarity, relevance, and structure. Reliability is tested using statistical methods, such as Cronbach's Alpha, to ensure the questionnaire items are internally consistent and that the instrument produces stable, consistent results over time. The collected data are analyzed using both descriptive and inferential statistical methods. Descriptive statistics, such as frequency distributions, percentages, mean score and standard deviation were used to summarize the data and describe patterns in cybersecurity threats and information security practices. Inferential statistics, particularly correlation analysis and regression analysis, are used to test the relationship between cybersecurity threats and information security management effectiveness, as well as to test the research hypotheses. This allows the study to determine whether there is a statistically significant relationship between the variables. Ethical

considerations are strictly observed throughout the research process. Respondents are assured of confidentiality and anonymity, and participation is voluntary. No personal identifiers are collected, and all data is used strictly for academic purposes. This is particularly important given the sensitivity of cybersecurity-related information in government institutions. Approval is also obtained from relevant institutional authorities before data collection begins to ensure compliance with administrative and ethical standards.

3. Results

Research Question 1: What are the major cybersecurity threats affecting government institutions within the FCT, Abuja?

Table 1: Major Cybersecurity Threats in Government Institutions (FCT Abuja)

Cybersecurity Threats	SA (5)	A (4)	N (3)	D (2)	SD (1)	Total	Mean	Decision
Malware attacks	120	90	40	30	20	300	3.93	Accepted
Phishing attacks	130	100	35	20	15	300	4.10	Accepted
Insider threats	110	95	50	25	20	300	3.87	Accepted
Ransomware attacks	115	85	45	35	20	300	3.83	Accepted
Data breaches	140	80	40	25	15	300	4.15	Accepted
DoS/DDoS attacks	100	90	60	30	20	300	3.73	Accepted

The results in Table 1 show that all listed cybersecurity threats are significant in government institutions within the FCT, Abuja, as all mean scores are above the benchmark of 3.00. Among the threats**,** data breaches (mean = 4.15) and phishing attacks (mean = 4.10) were the most prevalent, indicating that unauthorized access and social engineering attacks are the most common risks facing government digital systems. Malware and insider threats also recorded high mean values, showing that both external and internal vulnerabilities contribute significantly to cybersecurity risks. This implies that government institutions in Abuja are exposed to multiple layers of cyber threats, making their digital systems highly vulnerable without strong security controls.

Research Question 2: How effective are the information security management systems in government institutions within the FCT, Abuja?

Responses were analyzed using Likert-scale weighted means to determine the effectiveness of ISM practices.

Table 2: Effectiveness of Information Security Management Systems

Information Security Management Indicators	SA	A	N	D	SD	Total	Mean	Decision
Cybersecurity policy implementation	60	80	70	60	30	300	3.40	Moderate
Access control systems	70	85	60	55	30	300	3.53	Effective
Incident response mechanism	55	75	80	60	30	300	3.32	Moderate
Employee cybersecurity training	50	70	85	65	30	300	3.23	Weak
Encryption usage	65	90	70	45	30	300	3.55	Effective
Risk assessment practices	60	80	75	55	30	300	3.43	Moderate

The findings reveal that information security management systems in government institutions within the FCT, Abuja are moderately effective but not fully robust**.** Access control systems and encryption practices recorded relatively higher mean scores, indicating some level of technical protection within government ICT systems. However, employee cybersecurity training recorded the lowest mean score (3.23), showing that human capacity development remains a major weakness. Overall, the results suggest that while basic cybersecurity structures exist, they are not sufficiently strong to fully protect government systems against evolving cyber threats. This indicates a gap between policy formulation and effective implementation in Nigerian public institutions.

Hypothesis Testing

H_0: There is no significant relationship between cybersecurity threats and information security management effectiveness in government institutions within the FCT, Abuja.
H_1: There is a significant relationship between cybersecurity threats and information security management effectiveness in government institutions within the FCT, Abuja.

A Pearson Product Moment Correlation (PPMC) analysis was used to test the hypothesis at 0.05 level of significance.

Table 3: Correlation Analysis between Cybersecurity Threats and ISM Effectiveness

Variables	Mean	Std. Dev	N	r-calculated	p-value	Decision
Cybersecurity Threats	3.98	0.62	300	0.71	0.000	Significant
ISM Effectiveness	3.41	0.58	300			

The correlation analysis shows a strong positive relationship ($r = 0.71$, $p < 0.05$) between cybersecurity threats and information security management effectiveness in government institutions within the FCT, Abuja. This indicates that as cybersecurity threats increase, there is a corresponding increase in efforts toward improving information security management systems, although not at a sufficient level to eliminate vulnerabilities. Since the p-value (0.000) is less than

0.05, the null hypothesis (H_0) is rejected, while the alternative hypothesis (H_1) is accepted. This means that there is a statistically significant relationship between cybersecurity threats and information security management effectiveness in government institutions in Abuja. However, the strength of this relationship also suggests that despite existing security measures, institutions are still reactive rather than fully proactive in their cybersecurity approach, meaning that security improvements are often driven by the occurrence of threats rather than preventive planning.

4. Discussion of Findings

The findings from Table 1 clearly indicate that cybersecurity threats are not only present but highly prevalent within government institutions in the Federal Capital Territory (FCT), Abuja. The fact that all mean scores are above the benchmark of 3.00 confirms that respondents consistently experience and acknowledge multiple forms of cyber threats affecting their digital operations. The most dominant threats identified are data breaches (mean = 4.15) and phishing attacks (mean = 4.10), suggesting that government systems are particularly vulnerable to unauthorized access and human-targeted manipulation strategies. This finding aligns closely with Okechukwu's (2022) position**,** which argues that "data compromise in Nigerian public institutions is increasingly driven by weak authentication systems and poor user awareness rather than system failure alone." Similarly, Afolabi and Yusuf (2023) emphasize that phishing attacks have become the most successful attack vector in Nigerian MDAs due to "low cybersecurity awareness among employees and increasing reliance on email-based administrative communication." The prominence of malware and insider threats also reflects a dual-layer vulnerability within government institutions, external cyberattacks and internal human risks. This supports Chukwuemeka's (2021) argument that Nigerian government systems are exposed to "a hybrid of external cyber intrusion and internal negligence that together amplify institutional insecurity." In the same vein, Bello and Ibrahim (2024) observe that insider threats are increasingly difficult to detect in Abuja-based institutions because "employee access privileges are often poorly monitored and security audits are irregularly conducted." This demonstrates that cybersecurity challenges in the FCT are not isolated technical issues but systemic problems involving both human and technological weaknesses. The implications of these findings are that government institutions in Abuja operate in a high-risk digital environment where multiple cyber threats coexist and reinforce one another. This reinforces the view of Umar and Okafor (2023), who describe Nigeria's public sector cyber landscape as "an evolving threat ecosystem where attackers exploit both technological gaps and human vulnerabilities simultaneously." Therefore, the high prevalence of these threats indicates that existing cybersecurity frameworks are not sufficient to neutralize emerging risks in government digital systems.

The second finding reveals that information security management (ISM) systems in government institutions within the FCT, Abuja, are only moderately effective. While access control systems and encryption practices show relatively stronger performance, the overall system remains weak due to inadequate human capacity development and inconsistent implementation of cybersecurity policies. The low mean score for employee cybersecurity training (3.23) is particularly significant because it highlights a persistent human capital gap in Nigeria's cybersecurity ecosystem. This observation is strongly supported by Nwosu (2022), who argues

that “the weakest link in Nigeria’s cybersecurity architecture is not technology but human capacity deficiency.” Similarly, Eze and Mohammed (2024) emphasize that although Nigerian MDAs have adopted various cybersecurity tools, “the absence of continuous staff training significantly reduces the effectiveness of these tools in preventing cyber incidents.” This suggests that technological investments alone are insufficient without parallel investment in human capability development. The finding that ISM effectiveness is moderate rather than strong supports Adamu's (2023) argument that “most cybersecurity frameworks in Nigerian public institutions exist at the policy level but suffer serious implementation deficits at the operational level.” This gap between policy and practice is a recurring issue in Nigerian cybersecurity governance, particularly in Abuja, where institutional complexity often slows enforcement processes. Ibrahim and Bello (2025) further explain that “many government institutions in Nigeria possess cybersecurity policies, but lack structured monitoring systems to ensure compliance and accountability.” Overall, this indicates that ISM in the FCT is characterized by partial implementation, with technical controls in place but not fully supported by institutional culture, training, and enforcement mechanisms. This situation creates a reactive security environment rather than a preventive one.

The correlation result ($r = 0.71$, $p < 0.05$) indicates a strong, statistically significant relationship between cybersecurity threats and information security management effectiveness in government institutions in the FCT, Abuja. This implies that as cybersecurity threats increase, institutions tend to strengthen or adjust their information security management systems. However, the positive relationship does not necessarily indicate effectiveness in prevention; rather, it suggests adaptive or reactive improvements in response to increasing cyber incidents. This finding is consistent with the work of Ogunleye (2021), who explains that “cybersecurity development in Nigerian public institutions is largely incident-driven rather than prevention-driven.” In other words, security improvements often occur after an attack rather than as part of proactive risk management planning. Similarly, Bamidele and Kalu (2023) argue that Nigerian MDAs tend to “respond to cybersecurity threats only after operational disruption has occurred, thereby reinforcing a reactive security culture.” The rejection of the null hypothesis and acceptance of the alternative hypothesis further confirm that cybersecurity threats significantly influence the design and implementation of information security systems in Abuja-based government institutions. However, the strength of this relationship also exposes a critical limitation: institutions remain insufficiently proactive in anticipating and preventing cyber threats. Instead, they are largely driven by incident response and recovery strategies. This supports the conclusion of Okafor and Yusuf (2024), who state that “Nigeria’s cybersecurity posture remains largely defensive and reactive, with limited predictive and preventive capabilities across public sector institutions.” Therefore, while the relationship between cybersecurity threats and ISM effectiveness is statistically significant, it also highlights the need for stronger proactive governance frameworks, continuous training, and advanced threat intelligence systems.

5. Conclusion

This study examined cybersecurity threats and information security management in government institutions within the Federal Capital Territory (FCT), Abuja, with the aim of understanding the nature of cyber risks, assessing the effectiveness of security management

systems, and determining the relationship between both variables. Based on data collected from respondents across selected Ministries, Departments, and Agencies (MDAs), the study found that cybersecurity threats are highly prevalent and continuously evolving in the Nigerian public sector digital environment. The findings revealed that government institutions in Abuja are exposed to multiple categories of cyber threats, including data breaches, phishing attacks, malware infections, insider threats, and ransomware. These threats are not isolated but interconnected, often resulting from weak authentication systems, inadequate monitoring mechanisms, poor cybersecurity awareness among staff, and outdated technological infrastructure. The presence of these vulnerabilities indicates that government digital systems are operating in a high-risk cyber environment where both internal and external actors contribute to security compromise.

The study further concluded that information security management systems in these institutions are only moderately effective. While certain technical controls,, such as encryption mechanisms and access control systems, are in place, their effectiveness is weakened by poor implementation of cybersecurity policies, limited personnel training, and inadequate coordination among security units. This suggests that cybersecurity management in the FCT public sector is still in its early stages and has not fully matured to match the sophistication of emerging cyber threats. The study established a statistically significant relationship between cybersecurity threats and the effectiveness of information security management. This relationship indicates that as cyber threats increase, government institutions tend to respond by improving or adjusting their security systems. However, this response is largely reactive rather than proactive, meaning that cybersecurity improvements are often triggered by incidents rather than preventive planning. This reactive posture limits the overall resilience of government institutions against future cyberattacks.

6. Recommendations

Based on the study's findings, the following recommendations are made to improve cybersecurity resilience and information security management in government institutions in the FCT, Abuja.

1. Government institutions within the FCT, Abuja, should adopt a proactive cybersecurity strategy rather than relying on reactive responses to cyber incidents. This should include implementing continuous risk assessment frameworks, predictive threat-monitoring systems, and real-time security intelligence tools that detect and mitigate threats before they escalate into major cyberattacks. Such a preventive approach will significantly strengthen institutional resilience against evolving cyber threats.
2. There is a strong need for continuous cybersecurity training and capacity development for all staff across Ministries, Departments, and Agencies (MDAs). Since many cyber incidents are caused by human error and a lack of awareness, regular training programs, workshops, and simulated cyber-attack exercises should be institutionalized. This will equip employees with the knowledge to identify and respond effectively to threats such as phishing, social engineering, and credential theft.
3. Government institutions should strengthen the enforcement of existing cybersecurity policies by ensuring strict compliance across all departments. Policy implementation should be supported with effective monitoring and evaluation frameworks that track adherence to

cybersecurity standards. In addition, dedicated cybersecurity compliance units should be established within MDAs to ensure accountability, consistency, and enforcement of security protocols.

4. There is also a need for increased investment in modern cybersecurity infrastructure, including advanced firewalls, intrusion detection and prevention systems, secure cloud computing architectures, and multi-factor authentication systems. Many government systems are outdated and vulnerable to cyberattacks. Upgrading these systems will significantly reduce exposure to cyber threats and enhance data protection.
5. Inter-agency collaboration on cybersecurity matters should be improved to enable effective sharing of threat intelligence across all government institutions. A centralized cybersecurity coordination framework should be strengthened to quickly communicate incidents affecting one agency to others, thereby reducing the spread and impact of cyberattacks across the public sector.
6. The government should increase budgetary allocation for cybersecurity development in public institutions. Adequate funding is necessary to support infrastructure upgrades, staff training, cybersecurity research, and the deployment of advanced security technologies. Without sufficient financial investment, even well-designed cybersecurity policies will remain ineffective in practice.

REFERENCES

Abdullahi, M. (2021). Cybercrime and digital vulnerability in Nigerian public institutions. *Journal of Information Security and Governance*, 6(2), 45–60.

Abubakar, S. (2021). ICT infrastructure dependency and cybersecurity risks in Nigeria's public sector. *Nigerian Journal of Cyber Studies*, 4(1), 15–29.

Adegoke, T. (2023). Policy enforcement gaps in Nigeria's cybersecurity governance framework. *African Journal of Public Administration and Digital Security*, 8(3), 112–128.

Adamu, R. (2025). Cybersecurity workforce shortage and institutional resilience in Nigerian MDAs. *International Journal of Digital Governance in Africa*, 10(1), 33–50.

Afolabi, K. (2023). E-governance and cyber exposure in Nigerian federal institutions. *Journal of Public Sector ICT Development*, 7(2), 77–91.

Akinyemi, O. (2022). Digital transformation and cyber risk exposure in Nigerian governance systems. *Nigerian Journal of Information Technology and Security*, 5(1), 22–38.

Akinwale, F. (2022). Socio-technical challenges in Nigeria's digital governance systems. *Journal of African Technology and Society*, 3(2), 55–70.

Bamidele, J. (2024). Human capacity development and cybersecurity performance in public institutions. *Journal of ICT and Governance Studies*, 9(1), 41–58.

Bello, M., & Adeyemi, K. (2025). Cybersecurity governance and reactive security culture in Nigeria. *Journal of Information Systems Governance*, 11(1), 14–30.

Bello, R., & Yusuf, T. (2026). Inter-agency collaboration and cybersecurity intelligence sharing in Nigeria. *African Cybersecurity Review*, 12(1), 20–39.

Chinedu, U., & Aisha, M. (2022). E-governance systems and cyber vulnerability expansion in Nigeria. *Nigerian Journal of Digital Administration*, 6(1), 34–50.

Chukwu, E., & Eze, P. (2022). Insider threats and cybersecurity risks in Nigerian government institutions. *Journal of Information Risk Management*, 5(2), 58–73.

Danlami, H., & Ibrahim, Y. (2022). Digital migration and cyber vulnerability in public sector systems. *Journal of African Cybersecurity Studies*, 4(3), 45–63.

Danladi, M. (2021). Cybersecurity threats in Nigerian federal institutions: An empirical review. *Journal of ICT and National Security*, 3(1), 10–25.

Eze, C., & Ibrahim, L. (2024). Digital transformation and data security maturity in Nigerian MDAs. *International Journal of E-Governance and Security*, 9(2), 70–88.

Eze, P., & Mohammed, S. (2024). Cybersecurity readiness and institutional weaknesses in Nigeria. *African Journal of Cyber Policy*, 7(1), 25–41.

Eze, P., & Okoro, D. (2025). Socio-technical alignment and digital governance effectiveness in Nigeria. *Journal of Public Administration and Technology*, 10(2), 55–72.

Ibrahim, A., & Sani, M. (2023). Cybersecurity policy fragmentation in Nigerian MDAs. *Journal of African Public Sector ICT*, 6(2), 44–60.

Idris, A., & Okafor, C. (2024). Cybersecurity governance and trust in digital public systems. *African Journal of Digital Policy and Security*, 8(1), 19–35.

Kalu, P. (2023). Cloud computing adoption and cybersecurity risks in Nigeria. *Journal of Digital Infrastructure and Security*, 7(3), 60–78.

Mahmud, B., & Ibrahim, T. (2023). Information security governance challenges in Nigerian public institutions. *Journal of Governance and Cybersecurity*, 6(1), 28–44.

Nwafor, U., & Yakubu, A. (2025). Cybersecurity policy effectiveness and enforcement challenges In Nigeria. *Journal of African Digital Governance*, 10(2), 22–40.

Nwosu, C. (2023). Centralized cybersecurity governance and institutional silos in Nigeria. *Journal of Information Systems and Policy*, 7(1), 30–46.

Ogunleye, T. (2021). Cybersecurity governance structures in Nigeria's public sector. *Nigerian Journal of Information Security*, 4(2), 18–33.

Ogunleye, T. (2022). Policy implementation gaps in Nigeria's cybersecurity framework. *African Journal of Cyber Policy Studies*, 6(1), 15–32.

Okechukwu, F. (2021). Digital migration and cyber exposure in Nigerian public administration. *Journal of ICT and Governance*, 5(1), 11–27.

Okafor, C., & Bello, M. (2023). Cybercrime and institutional credibility in Nigeria. *Journal of Public Sector Security Studies*, 7(2), 50–68.

Okonkwo, J., & Bello, A. (2023). E-governance expansion and cyber risk exposure in Nigeria. *Journal of Digital Policy and Security Studies*, 6(3), 35–52.

Olatunji, K. (2024). Data integrity challenges in Nigerian government information systems. *Journal of Information Assurance and Security*, 9(1), 44–61.

Ojo, R., & Mohammed, S. (2022). Cyber threats in Nigerian public institutions: A field study. *Journal of African Cyber Studies*, 5(2), 20–37.

Suleiman, A. (2024). Cybersecurity governance enforcement and compliance in Nigeria. *International Journal of Public Sector Security*, 8(2), 38–55.

Umar, H., & Chukwuemeka, P. (2023). Cybersecurity breaches and governance weaknesses in Nigeria. *Journal of Cyber Risk and Policy*, 6(2), 27–43.

Umaru, I. (2024). Cyber insecurity and national security implications in Nigeria. *Journal of Security and Strategic Studies*, 10(1), 12–29.

Usman, A., & Bello, K. (2024). Cyber threat attractiveness of Nigeria's Federal Capital Territory. *Journal of African Security Studies*, 7(1), 33–48.

Yakubu, M., & Adesina, R. (2022). Cybersecurity policy adoption and enforcement gaps in Nigerian MDAs. *Journal of Information Governance in Africa*, 5(3), 41–58.