



Human Resource Management Practices and Cybersecurity Risk Mitigation in Public Sector E-Services: Lessons from Nigeria

* **Dr. Arumede, Martin Uhwo**

Department of Public Administration and Local Government, University of Nigeria, Nsukka, Nigeria.
E-mail: martin.arumede@unn.edu.ng

Submission Date: 16 July 2026 **Published Date:** 24 Sept. 2026

Citation: Arumede, M. U. (2026). Human Resource Management Practices and Cybersecurity Risk Mitigation in Public Sector E-Services: Lessons from Nigeria. In INSR Journal of Multidisciplinary Studies (Vol. 2, Number 9, pp. 88–94). <https://doi.org/10.5281/zenodo.22940342>

Corresponding author: **Dr. Arumede, Martin Uhwo**

Department of Public Administration and Local Government, University of Nigeria, Nsukka, Nigeria.

Copyright: © 2026 Dr. Arumede, Martin Uhwo. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 international License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract

The digitization of public service delivery in Nigeria through e-government platforms such as Treasury Single Account (TSA), Integrated Payroll and Personnel Information (IPPIS), and citizen portals has increased exposure to cybersecurity risks. While technology is critical, employees remain the weakest link in the cybersecurity chain. This study examines how Human Resource Management [HRM] practices contribute to cybersecurity risk mitigation in Nigerian public sector e-services. Anchored on Human Capital Theory, the study adopts a qualitative approach using secondary data and content analysis of government reports, NITDA, OAGF, and academic publications from 2022 to 2024. Findings reveal that cybersecurity training and development, security-focused recruitment and selection, and performance appraisal with cybersecurity key performance indicators (KPIs) significantly reduce human-related cyber incidents. The study concludes that strategic HRM practices are essential for building a cyber-resilient public workforce and sustaining trust in digital governance.

Keywords: HRM practices, cybersecurity, risk mitigation, public sector, e-services, Nigeria, training and development, human capital.

Introduction

The digital transformation of public service delivery in Sub-Saharan Africa has accelerated rapidly since 2020, with e-government platforms becoming central to revenue collection, citizen registration, health, and social welfare programs. In Nigeria, initiatives such as the Nigeria Inter-Bank Settlement System, IPPIS, and various state e-portals have expanded access but also increased exposure to cyber threats (NITDA, 2023). This shift means that cybersecurity is no longer just an ICT issue but a core governance and human resource challenge for the public sector. Human Resource Management plays a critical role in mitigating cybersecurity risks because employees are consistently identified as the weakest link in information security. Insider threats, phishing, poor password hygiene, and lack of awareness account for over 70% of breaches in public institutions globally (IBM, 2024). Therefore, HRM practices such as recruitment, training, performance management, and policy enforcement directly shape the cybersecurity posture of government agencies. In the Nigerian public sector, the adoption of e-services has outpaced the development of corresponding HR capacity. Many MDAs still operate with HR policies designed for manual processes and lack cybersecurity competencies in job descriptions and performance metrics (OECD, 2023). This creates a gap where technical controls exist but human vulnerabilities remain unaddressed, making HRM a strategic lever for risk reduction.

The National Cybersecurity Policy and Strategy 2021 and the Nigeria Data Protection Act 2023 both emphasize the need for human capacity development as a pillar of national cyber resilience (NITDA, 2023). However, implementation at MDA level is fragmented. Without HRM embedding cybersecurity into recruitment, onboarding, and continuous development, policies remain aspirational rather than operational. Globally, public sector organizations are repositioning HRM as a cybersecurity function. Studies show that agencies with cybersecurity-aware HR practices experience fewer incidents and faster incident response (Deloitte, 2024). Practices such as role-based security training, cyber risk screening during hiring, and linking performance appraisal to compliance have become standard in OECD countries.

In Nigeria, the challenge is compounded by high staff turnover, limited cybersecurity expertise, and competing priorities. The Office of the Head of Civil Service (2024) notes that many public servants lack basic digital literacy, let alone cybersecurity awareness. This increases susceptibility to social engineering and data breaches in e-service platforms that handle sensitive citizen data. Training and development is emerging as the most direct HRM intervention. NITDA (2023) launched the National Cybersecurity Awareness Program targeting public servants, but coverage remains low. Effective training must move beyond one-off workshops to continuous, role-specific learning embedded in HR processes to build a security culture (SANS Institute, 2024). Recruitment and selection is another critical entry point. Integrating cybersecurity competencies into job analysis and selection criteria ensures that new hires understand data protection and risk responsibilities from day one (SHRM, 2023). In Nigeria, civil service recruitment still prioritizes academic qualifications over digital and security competencies, creating capability gaps. Performance management and accountability mechanisms are also vital. When cybersecurity KPIs are included in performance contracts, employees are more likely to comply with policies (World Bank, 2024). Conversely, the absence of consequences for violations weakens risk mitigation efforts in many Nigerian MDAs. Given these dynamics, this study examines how HRM practices can be leveraged to mitigate cybersecurity risks in public sector e-services in Nigeria. It draws lessons from policy, training, recruitment, and organizational culture to propose an HR-driven model for building cyber-resilient public institutions (NITDA, 2023; IBM, 2024).

Statement of the Problem

Nigeria's public sector has invested heavily in e-government platforms to improve service delivery and transparency. However, the frequency and impact of cyberattacks on government systems have also increased, with NITDA (2023) reporting over 2,000 cybersecurity incidents in public institutions in 2023 alone. Many of these incidents are traced to human error rather than technical failure. Despite the existence of national cybersecurity frameworks, implementation at the MDA level remains weak. The Nigeria Data Protection Act (2023) mandates data protection officers and staff training, but compliance is low due to lack of enforcement and HR capacity (NITDA, 2023). This creates a situation where policies exist on paper but are not operationalized. Human Resource Management in the Nigerian civil service has not fully integrated cybersecurity into its core functions. Recruitment processes rarely assess digital security competencies, and job descriptions seldom include cybersecurity responsibilities (OECD, 2023). As a result, employees are hired and deployed to manage e-services without adequate risk awareness.

Training and development programs are ad hoc and not aligned with emerging cyber threats. Most cybersecurity training in MDAs is project-based and donor-driven, rather than institutionalized in HR policy (Office of the Head of Civil Service, 2024). This leads to low retention of knowledge and poor security behavior among staff. There is also a gap in accountability. Performance appraisal systems in the public sector do not include cybersecurity compliance as a metric (World Bank, 2024). Without linking behavior to rewards or sanctions, employees have little incentive to follow security protocols, increasing organizational vulnerability. The cost of cyber incidents to the Nigerian government is rising. IBM (2024) estimates that the average cost of a data breach in Africa is \$2.9 million, with public sector breaches often leading to loss of citizen trust and disruption of services. The human factor remains the most exploited vector, yet HRM is rarely involved in incident response or risk planning.

Existing literature on cybersecurity in Nigeria focuses largely on technical solutions and ICT policy, with limited attention to the role of HRM (NITDA, 2023). This leaves a critical gap in understanding how people-centered interventions can reduce risk in e-government. Therefore, this study seeks to address the problem of how HRM practices — recruitment, training, performance management, and policy enforcement — can be strategically used to mitigate cybersecurity risks in Nigerian public sector e-services, and what lessons can be drawn for building a cyber-aware public workforce.

Research Questions

1. How do HRM practices contribute to cybersecurity risk mitigation in Nigerian public sector e-services?
2. To what extent does cybersecurity training and development reduce human-related cyber incidents in public institutions?
3. How do recruitment, selection, and performance appraisal influence employees' cybersecurity behavior in the public sector?

Objectives of the Study

The broad objective of the study is to examine the role of HRM practices in mitigating cybersecurity risks in public sector e-services in Nigeria. While the specific Objectives are as follows:

1. To assess the impact of cybersecurity training and development on employee cyber behavior in public institutions.
2. To examine how security-focused recruitment and selection influence cybersecurity risk levels.
3. To evaluate the role of performance appraisal with cybersecurity KPIs in promoting secure practices.

Hypotheses

1. Cybersecurity training and development programs significantly reduce human-related cybersecurity incidents in Nigerian public institutions.
2. Security-focused recruitment and selection practices are positively related to lower cybersecurity risks in public sector e-services.
3. Inclusion of cybersecurity KPIs in performance appraisal significantly improves employees' compliance with cybersecurity policies.

Literature Review

HRM and Cybersecurity in the Public Sector

Human Resource Management is increasingly recognized as a frontline defense in cybersecurity. In the public sector, where large volumes of citizen data are processed, HRM ensures that the right people with the right skills and security mindset are hired and retained (SHRM, 2023). This human-centric approach complements technical controls. One key area is policy development and enforcement. HR departments are responsible for developing acceptable use policies, data protection guidelines, and disciplinary procedures related to cybersecurity (Deloitte, 2024). In Nigeria, NITDA (2023) recommends that every MDA have an HR-led cybersecurity policy, but adoption is inconsistent. HRM also manages access control through onboarding and offboarding processes. Proper account provisioning and timely deactivation of access for exiting staff are critical to prevent insider threats (IBM, 2024). Weak offboarding in many Nigerian MDAs has been linked to unauthorized access incidents. Employee awareness and culture building is another HRM function. A security-aware culture reduces risky behaviors such as clicking phishing links or sharing passwords (SANS Institute, 2024). HRM can drive this through communication campaigns, induction programs, and leadership modeling. Performance management systems can integrate cybersecurity KPIs. When employees are evaluated on compliance with data protection and information security protocols, adherence improves (World Bank, 2024). This is currently missing in most Nigerian public sector appraisal systems. Incident response also requires HR involvement. HR must manage communications, support staff affected by breaches, and ensure lessons are captured for training (OECD, 2023). Without HR, technical teams handle incidents in isolation, missing the human dimension.

Risk assessment and workforce planning should include cyber risk. HRM needs to identify critical roles with access to sensitive data and ensure they have appropriate vetting and training (NITDA, 2023). This is particularly important for e-service platforms handling financial and health data. HRM and cybersecurity are converging. For public sector e-services to be resilient, HRM must be treated as a strategic partner in cybersecurity governance, not just an administrative function (Deloitte, 2024). Training and development is the most direct HRM tool for reducing human-related cyber risks. Because most breaches start with employee mistakes, continuous learning is essential (IBM, 2024). In the public sector, this means moving beyond generic ICT training to cybersecurity-specific programs. NITDA (2023) launched the National Cybersecurity Awareness Program to train public servants, but reach and frequency are limited. Effective programs must be role-based, with different content for executives, IT staff, and general users handling citizen data. Adult learning principles suggest that training must be continuous and contextual. One-off workshops have little impact on behavior change (SANS Institute, 2024). Microlearning, simulations, and phishing drills have been shown to significantly reduce click rates in government agencies (Deloitte, 2024).

Training should be embedded in the employee lifecycle. Onboarding must include cybersecurity orientation, while annual refresher courses address new threats (SHRM, 2023). This ensures knowledge remains current as attack methods evolve. Evaluation is critical. Training effectiveness should be measured through behavior change, incident rates, and compliance audits, not just attendance (World Bank, 2024). Many Nigerian MDAs lack mechanisms to assess whether training translates to safer practices. Leadership training is equally important. Managers must understand their role in enforcing security policies and modeling good behavior (OECD, 2023). Without leadership buy-in, staff training has limited impact. Partnerships can bridge capacity gaps. Collaborations between NITDA, universities, and private sector can provide scalable training content and certification for public servants (NITDA, 2023). This reduces cost and improves quality. Training and development must be institutionalized as a core HRM function. It is the most cost-effective way to build a human firewall in public sector e-services and mitigate cybersecurity risks (IBM, 2024; SANS Institute, 2024).

Recruitment and Selection for Cybersecurity

Recruitment and selection are the first opportunity to build cybersecurity resilience. Hiring people with the right security mindset reduces long-term risk (SHRM, 2023). For public sector e-services, this means defining cybersecurity competencies in job descriptions. Job analysis should identify roles with access to sensitive data and specify required cybersecurity knowledge (OECD, 2023). In Nigeria, many e-service roles still do not include security responsibilities in their job profiles, creating ambiguity. Selection processes can include cybersecurity assessments. This may involve scenario-based questions, basic digital literacy tests, or background checks for sensitive positions (Deloitte, 2024). Such practices are common in financial institutions but rare in Nigerian MDAs. Vetting is important for insider risk mitigation. Background checks and reference verification help prevent hiring individuals with a history of data misuse (IBM, 2024). The Nigerian public service recruitment process needs stronger vetting for IT and data-handling roles. Onboarding is an extension of selection. New hires should receive cybersecurity orientation and sign acceptable use agreements before accessing systems (NITDA, 2023). This sets expectations from day one. Diversity in recruitment also matters. Teams with varied skills are better at identifying risks and designing secure processes (World Bank, 2024). HRM should therefore avoid hiring only technical staff and include behavioral and policy expertise. Automation of recruitment can help. E-recruitment platforms can screen for cybersecurity certifications and include mandatory security training modules (SHRM, 2023). This is yet to be widely adopted in Nigeria. Strategic recruitment and selection can prevent many cybersecurity problems before they occur. By embedding security into hiring, public sector organizations build a workforce that is part of the solution (Deloitte, 2024).

Theoretical Framework

Human Capital Theory

Human Capital Theory, advanced by Becker (1964) and Schultz (1961), posits that investments in education, training, and skills development increase individual productivity and organizational performance. In the context of cybersecurity, human capital refers to the knowledge, skills, and security awareness that employees bring to protect organizational assets. Recent applications of the theory emphasize that cybersecurity is a form of organizational capability that must be deliberately built through HRM investments (Deloitte, 2024). In the public sector, Human Capital Theory suggests that governments that invest in cybersecurity training, recruitment of skilled personnel, and continuous development will have lower breach rates and more resilient e-service systems (OECD, 2023). This is particularly relevant for Nigeria, where the digital skills gap in the civil service undermines cybersecurity efforts (NITDA, 2023). The theory provides a framework for understanding HRM practices as strategic investments rather than costs.

Gap in Literature

Despite growing interest in cybersecurity in Nigeria, most studies focus on technical controls, ICT policy, and legal frameworks, with limited attention to the role of Human Resource Management (NITDA, 2023; IBM, 2024). Existing literature rarely examines how recruitment, training, and performance management practices specifically contribute to cybersecurity risk mitigation in public sector e-services. This leaves a gap in understanding the human factors that drive security outcomes in government.

Furthermore, there is little empirical research on how Nigerian public sector organizations are integrating cybersecurity into HRM processes. Most available reports are either global best practice guides or technical audits, with no contextual analysis of civil service structures and capacity constraints (OECD, 2023; Office of the Head of Civil Service, 2024). This study therefore fills the gap by providing lessons from Nigeria on how HRM practices can be leveraged to build cyber-resilient public institutions.

Methodology

This study adopted a qualitative research design. It relied on secondary data sourced from NITDA reports, OAGF audit reports, CBN guidelines, academic journals, and publications by IBM, Deloitte, World Bank, and UNDP between 2022 and 2024. Content analysis was used to analyze the data. This involved identifying, coding, and categorizing themes related to HRM practices and cybersecurity outcomes in Nigerian public institutions (Krippendorff, 2013).

Discussion of Hypotheses

H1: Cybersecurity training and development programs significantly reduce human-related cybersecurity incidents in Nigerian public institutions

Human error accounts for over 70% of cybersecurity breaches in organizations globally, making employee behavior a critical risk factor (IBM, 2024). In Nigerian public institutions, where e-services have expanded rapidly, staff often lack the basic knowledge to identify phishing, social engineering, and password risks. This makes training and development a primary intervention for risk mitigation (NITDA, 2023). The National Cybersecurity Policy and Strategy 2021 identifies human capacity development as one of its five pillars. NITDA (2023) launched the National Cybersecurity Awareness Program targeting MDAs, but coverage remains below 30% of federal employees. Where training has been implemented, agencies report a decline in successful phishing attempts, suggesting a direct relationship between training and incident reduction. Adult learning theory supports continuous and contextual training over one-off workshops. SANS Institute (2024) found that organizations that conduct quarterly phishing simulations and microlearning modules experience 60% fewer click-through rates. This approach is more effective than annual seminars, which are common in Nigerian MDAs (Office of the Head of Civil Service, 2024).

Role-based training is particularly important. Employees handling financial data, citizen health records, or procurement systems face different threats and require tailored content (Deloitte, 2024). Generic ICT training does not address these nuances, which explains why many Nigerian public servants still fall for targeted attacks despite attending general digital literacy programs. Evaluation of training effectiveness is often missing. World Bank (2024) notes that public sector training programs in Africa rarely measure behavior change, focusing instead on attendance. Without post-training assessments and incident tracking, MDAs cannot determine if training translates to safer practices, limiting the impact of investments. Leadership involvement strengthens training outcomes. When senior management participates in cybersecurity training and communicates its importance, employee compliance improves (OECD, 2023). In Nigeria, cybersecurity is often delegated to ICT units with little executive sponsorship, weakening the cultural impact of training programs.

Partnerships can address resource constraints. Collaborations between NITDA, universities, and private cybersecurity firms can provide scalable, certified training at lower cost (NITDA, 2023). Such models have worked in Ghana and Kenya, where public-private training hubs increased civil servant certification rates by 40% within two years. Behavioral change takes time. SHRM (2023) emphasizes that security culture is built through repeated exposure, reinforcement, and feedback. Nigerian institutions that institutionalized monthly security tips and incident debriefs saw sustained improvements in password hygiene and reporting of suspicious emails. Cost-benefit analysis also supports training. IBM (2024) estimates that the average cost of a data breach in Africa is \$2.9 million, while the cost of comprehensive annual training per employee is less than \$200. For budget-constrained MDAs, training offers one of the highest returns on investment for risk reduction. The above discussion supports that cybersecurity training and development programs significantly reduce human-related cybersecurity incidents in Nigerian public institutions.

H2: Security-focused recruitment and selection practices are positively related to lower cybersecurity risks in public sector e-services

Recruitment is the first line of defense in cybersecurity. Hiring individuals with the right skills and security mindset reduces the likelihood of insider threats and policy violations (SHRM, 2023). In Nigerian public sector e-services, where access to sensitive citizen data is widespread, this is a strategic imperative. Job analysis and design must explicitly include cybersecurity responsibilities. OECD (2023) recommends that all roles with access to government databases specify security requirements. In Nigeria, most civil service job descriptions still focus on academic qualifications and years of experience, omitting digital security competencies (Office of the Head of Civil Service, 2024). Selection tools can assess security awareness. Scenario-based interview questions, basic digital literacy tests, and integrity checks help identify candidates who understand risk (Deloitte, 2024). Financial sector institutions in Nigeria have adopted these tools and reported lower fraud rates, but MDAs lag behind.

Background checks and vetting are critical for roles with privileged access. IBM (2024) found that 22% of insider incidents involved employees with prior disciplinary issues. Strengthening vetting in recruitment for IT, finance, and data management roles in Nigerian MDAs can reduce this risk. Onboarding is an extension of selection. NITDA (2023) mandates that new public servants receive cybersecurity orientation and sign data protection agreements. Implementation is inconsistent, with many employees gaining system access before receiving any security training. Competency-based hiring improves fit. SHRM (2023) argues that matching candidates' skills to job-specific security requirements reduces errors and increases policy compliance. For e-service roles in Nigeria, this means prioritizing candidates with certifications in data protection and information security. Diversity in hiring teams also matters. Teams with mixed technical and behavioral expertise are better at identifying risky hiring decisions (World Bank, 2024). Overreliance on technical hiring panels in Nigerian MDAs often overlooks behavioral risk factors.

Automation can improve screening. E-recruitment platforms can filter for cybersecurity certifications and flag applicants without required competencies (Deloitte, 2024). Nigeria's IPPIS recruitment portal does not currently have this functionality, representing a missed opportunity. Probationary periods should include security performance reviews. Evaluating new hires on compliance during the first six months helps identify risky behavior early (OECD, 2023). This is not standard practice in the Nigerian civil service. The analysis above support the hypothesis which states that security-focused recruitment and selection practices are positively related to lower cybersecurity risks in public sector e-services.

H3: Inclusion of cybersecurity KPIs in performance appraisal significantly improves employees' compliance with cybersecurity policies

What gets measured gets managed. Linking cybersecurity to performance appraisal creates accountability and signals organizational priority (World Bank, 2024). In Nigerian public institutions, where compliance is often voluntary, this is a powerful motivator. Current appraisal systems in the Nigerian civil service focus on output targets with no mention of information security (Office of the Head of Civil Service, 2024). This sends an implicit message that cybersecurity is not part of an employee's core job, leading to poor adherence to policies. Research shows that when security behaviors are included in KPIs, incident rates decline. Deloitte (2024) found that government agencies that added "adherence to data protection policy" to performance contracts reduced policy violations by 35% within one year. KPIs must be specific and measurable. Examples include: completion of annual cybersecurity training, reporting of phishing emails, zero password sharing incidents, and compliance with access control procedures (SANS Institute, 2024). Vague goals like "be security conscious" are ineffective.

Feedback loops are essential. Regular performance discussions that include cybersecurity feedback reinforce desired behavior (SHRM, 2023). Annual appraisals alone are insufficient; quarterly check-ins yield better results. Rewards and sanctions must be applied consistently. OECD (2023) notes that employees comply more when they see that security compliance affects promotions and bonuses, and that violations have consequences. In Nigeria, lack of enforcement undermines policy effectiveness. Leadership modeling influences appraisal outcomes. When managers are also evaluated on cybersecurity leadership, they are more likely to enforce policies with their teams (IBM, 2024). This creates cascading accountability. Technology can support monitoring. Security awareness platforms can automatically track training completion and phishing simulation results for inclusion in appraisals (Deloitte, 2024). This reduces administrative burden on HR. Cultural change takes time. SHRM (2023) emphasizes that linking KPIs to cybersecurity must be accompanied by communication and training, otherwise employees may perceive it as punitive. From the discussion above, we accept the hypothesis which states that inclusion of cybersecurity KPIs in performance appraisal significantly improves employees' compliance with cybersecurity policies.

Findings

1. Human error is the dominant cause of cybersecurity incidents in Nigerian public institutions, with phishing, poor password practices, and lack of awareness responsible for the majority of breaches reported by NITDA.
2. Cybersecurity training and development programs are fragmented and ad hoc in most MDAs. Where continuous, role-based training exists, there is a measurable reduction in successful attacks.
3. Recruitment and selection processes in the Nigerian public sector do not adequately assess cybersecurity competencies. Job descriptions and vetting procedures rarely include security requirements, increasing insider risk.
4. Performance appraisal systems exclude cybersecurity metrics. The absence of KPIs means employees have little incentive to comply with security policies, resulting in low adherence.
5. Leadership commitment and HR involvement are weak. Cybersecurity is largely treated as an ICT function, with HRM playing minimal role in policy enforcement, culture building, and risk management.
6. National policies exist but implementation at MDA level is poor. The Nigeria Data Protection Act (2023) and NITDA guidelines are not fully operationalized due to capacity and accountability gaps in HRM processes.

Recommendations

1. Continuous Institutionalization of role-based cybersecurity training for all public servants. NITDA and Head of Service should mandate quarterly training, phishing simulations, and behavior-based evaluation to reduce human error.
2. Revise recruitment and selection frameworks to include cybersecurity competencies: Job descriptions, interviews, and background checks should assess security awareness, especially for e-service roles.
3. Integrate cybersecurity KPIs into performance appraisal systems: MDAs should measure training completion, policy compliance, and incident reporting, and link results to rewards and promotions.
4. Position HRM as a strategic partner in cybersecurity governance: HR departments should lead policy communication, onboarding security orientation, and incident response support.
5. Strengthen leadership commitment through executive training and accountability: Senior managers should be evaluated on their role in promoting cybersecurity culture and compliance.
6. Leverage partnerships to build capacity: Government should collaborate with NITDA, universities, and private firms to deliver scalable, certified training and develop e-recruitment tools with security screening.

Conclusion

This study demonstrates that Human Resource Management practices are central to mitigating cybersecurity risks in Nigerian public sector e-services. Cybersecurity is not solely a technical problem; it is a human and organizational challenge. The findings confirm that training and development, security-focused recruitment, and performance management with cybersecurity KPIs significantly influence employee behavior and reduce incidents. Where these HRM practices are absent or weak, technical controls alone cannot protect government systems and citizen data. For Nigeria to achieve cyber resilience in public service delivery, a paradigm shift is required. Cybersecurity must be embedded into HR policies, processes, and culture. By investing in people through strategic HRM, Nigerian public institutions can build a workforce that acts as the first line of defense. The recommendations provided offer a practical roadmap for MDAs to transition from reactive technical fixes to proactive, people-centered cybersecurity risk management.

References

1. Adeyemi, S., & Bello, T. (2024). Capacity building for cybersecurity in Nigerian public institutions. *African Journal of Public Administration*, 18(1), 45–62.
2. Deloitte. (2024). 2024 Government cybersecurity outlook: Building a cyber-aware public workforce. Deloitte Insights.
3. Chukwu, O. N. (2023). Insider threats and HR risk management in the public sector. *International Journal of Human Resource Studies*, 13(3), 112–129.
4. Edwin, I. E., Odanwu, A. I., Okoli, J. (2024). Human resource management as a cyber security enabler in Nigeria: An exploratory approach. *World Journal of Economics, Business and Management*. Vol. 1, No. 1, 2024 Website: <https://wasrpublication.com/wjebm>
5. Eze, C. (2023). Digital literacy and cybersecurity awareness among Nigerian civil servants. *Nigerian Journal of Computer Science*, 9(4), 88–101.
6. IBM. (2024). Cost of a data breach report 2024. IBM Security.
7. Kumar, R., & Singh, P. (2023). HR practices and cybersecurity compliance in public organizations. *Journal of Information Security and Applications*, 72, 103432.
8. Mensah, I. K. (2023). E-government implementation and cybersecurity challenges in West Africa. *Government Information Quarterly*, 40(2), 101789.
9. National Information Technology Development Agency [NITDA]. (2023). National Cybersecurity Policy and Strategy 2021-2025: Implementation report. NITDA.
10. Nigeria Data Protection Commission. (2023). Nigeria Data Protection Act, 2023. Federal Government of Nigeria.
11. Office of the Head of Civil Service of the Federation. (2024). _Federal civil service strategy and implementation plan 2021-2025: Mid-term review. OHCSF.
12. Olayinka, D. (2024). Performance management and information security behavior in government agencies. *Public Personnel Management*, 53(2), 201–218.
13. Organisation for Economic Co-operation and Development [OECD]. (2023). Digital government in Nigeria: Strengthening public sector capacity for cybersecurity. OECD Publishing.
14. SANS Institute. (2024). _Security awareness report: Measuring and managing human risk. SANS.
15. Schultz, T. W. (1961). Investment in human capital. *The American Economic Review*, 51(1), 1–17.
16. Society for Human Resource Management [SHRM]. (2023). Managing cybersecurity risk through HR: A guide for HR professionals. SHRM.
17. World Bank. (2024). _Digital development report: Harnessing human capital for cyber resilience in Africa. World Bank Group.