A PUBLICATION OF WORD ASTRA
wordastrajournals@gmail.com
www.wordastrajournals.com

Global Journal of Modern Research and Emerging Trends (GJMRET)
Vol. 2, Issue 4, July 2026 - ISSN: 1595-076X

Cybersecurity and Information Management in Digital Libraries: Emerging Challenges for Nigerian Academic Institutions

[1]Nsikak Stephen Edet, Ph.D & [2]Ekwere Oluwatosin Emmanuel
[1]Department of Political Science, University of Uyo, Nigeria.
[2]Department of Library and Management Science
Abia State University, Nigeria
[1]nsikakstephen@yahoo.com, 08069212110
[2]oluwatosinsangodeyi@gmail.com, 08162413084

DOI: https://doi.org/10.67487/gjmret.v2i4.245

Citation: Edet, N. S., Emmanuel, E. O. (2026). Cybersecurity and Information Management in Digital Libraries: Emerging Challenges for Nigerian Academic Institutions. *Global Journal of Modern Research and Emerging Trends*, *2(4)*

Abstract

The progressive digitisation of library services in Nigerian academic institutions has created unprecedented opportunities for knowledge access while simultaneously exposing institutional information systems to an expanding and increasingly sophisticated landscape of cybersecurity threats. This study examines cybersecurity and information management in digital libraries of Nigerian universities, with a specific focus on the emerging challenges, policy frameworks, institutional responses, and prospects for sustainable security governance. Drawing on a systematic review of peer-reviewed scholarship, policy documents, and institutional assessments published between 2019 and 2025, the study evaluates the strengths and weaknesses of current cybersecurity practices and information management strategies in Nigerian academic libraries; assesses the adequacy of the national policy environment, including the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 (as amended in 2024), the Nigeria Data Protection Act (NDPA) of 2023, and relevant NITDA guidelines; and identifies the structural, institutional, and human capital factors that shape cybersecurity outcomes. Findings

indicate that Nigerian academic libraries face a complex threat matrix encompassing computer viruses, hacking, and unauthorised access to information resources, phishing, ransomware, insider threats, and social engineering attacks. These threats are compounded by structural vulnerabilities such as inadequate funding, erratic electricity supply, insufficient ICT infrastructure, an acute shortage of trained cybersecurity personnel, and the absence of institution-specific cybersecurity policies in most universities. While the national policy framework has been progressively strengthened, culminating in the comprehensive NDPA of 2023 and the amendment of the Cybercrimes Act in February 2024, its translation into effective institutional practice in academic library settings has been slow and uneven. The study is anchored in four theoretical frameworks; the Confidentiality, Integrity, and Availability (CIA) Triad Model, Information Security Management Systems (ISMS) theory, Routine Activity theory, and the Socio-Technical Systems Theory. Seven substantive policy recommendations are advanced for strengthening cybersecurity governance and information management in Nigerian academic digital libraries.

Keywords: cybersecurity, digital libraries, information management, Nigerian universities, academic institutions, data protection, cyberthreats, NDPA, policy implementation

1.1 Introduction

University libraries occupy a foundational position in the intellectual architecture of higher education. They serve as custodians of accumulated knowledge, repositories of primary research outputs, gateways to global information networks, and service platforms for faculty, students, and researchers. In Nigeria, Africa's most populous country, with over 170 accredited universities and a rapidly expanding higher education enrolment (National Universities Commission, 2024), academic libraries have undergone transformative digitisation over the past two decades, moving from predominantly print-based collections toward hybrid and increasingly fully digital library environments.

This digital transition has been both necessary and consequential. It has expanded access to research literature, enabled institutional repositories, facilitated distance learning, and connected Nigerian scholars to the global academic information ecosystem. Platforms

such as electronic databases, online public access catalogues (OPACs), institutional repositories, and digital resource management systems have become central to how Nigerian universities generate, preserve, and disseminate scholarly knowledge. Yet this transition has also introduced a class of vulnerabilities that traditional library security frameworks were not designed to address cybersecurity threats.

Globally, libraries and academic institutions have become increasingly attractive targets for cybercriminals. The British Library's catastrophic ransomware attack of October 2023, which destroyed significant portions of its digital infrastructure and took months to recover from, underscored the severity of cyber risk for information institutions even in highly resourced environments (Igbinovia & Ishola, 2023). In Nigeria, the threat landscape is compounded by structural factors; an unreliable electricity supply that disrupts continuous system monitoring; chronic underfunding of university libraries relative to their operational needs; a national shortage of qualified information technology and cybersecurity professionals; and a rapidly evolving threat environment in which cybercrime incidents reported to the Nigerian Cybercrime Advisory Council rose by 40 per cent between 2020 and 2023 (Nigerian Cyber Security Report, 2023).

Against this backdrop, the management of cybersecurity in Nigerian academic digital libraries has emerged as a critical institutional governance challenge. The adequacy of national policy frameworks including the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 (as amended in 2024); the Nigeria Data Protection Act (NDPA) of 2023, which superseded the Nigeria Data Protection Regulation (NDPR) of 2019; and NITDA's various guidelines, has improved over time, but the gap between national policy intent and actual institutional implementation in university library settings remains wide and consequential. This study critically examines this gap, assesses the strengths and weaknesses of current practices, and advances evidence-based recommendations for improvement.

1.2 Statement of the Problem

Despite the rapid expansion of digital library systems across Nigerian academic institutions, the cybersecurity and information management frameworks governing these systems remain fragmented, underdeveloped, and inadequately resourced. Several interconnected problems define this challenge.

First, the threat environment confronting Nigerian academic digital libraries has grown substantially more complex and damaging. Studies conducted across Nigerian universities consistently identify computer viruses as the most prevalent cyberthreat, followed by hacking, unauthorised access to information resources, password sniffing, and

impersonation. More sophisticated threats, including ransomware, Distributed Denial of Service (DDoS) attacks, phishing schemes, and insider threats, are increasingly being recorded, with ransomware incidents reported across Nigerian institutional settings rising by 287 per cent between 2020 and 2024. The consequences of successful cyberattacks on digital libraries are severe including data corruption, loss of irreplaceable research materials, disruption of academic services, exposure of sensitive patron personal data, and reputational damage to institutions.

Second, the institutional capacity to respond to these threats is critically deficient in most Nigerian universities. Research consistently documents inadequate training of library staff on cybersecurity measures, insufficient funding for security infrastructure, erratic power supply that disrupts system continuity, absence of institution-specific cybersecurity policies, and over-reliance on outdated or unlicensed security software. A survey of university libraries in South-East Nigeria found that most libraries lacked dedicated information security personnel and had not developed or implemented formal cybersecurity policies. Studies of institutional repositories in Nigerian universities similarly documented high levels of vulnerability to virus attacks and cyber hacks.

Third, while Nigeria's national cybersecurity and data protection policy framework has been progressively strengthened through the NDPR (2019), the NDPA (2023), the amended Cybercrimes Act (2024), and NITDA's institutional guidelines, the translation of these national instruments into specific, operationalised policies and security protocols for academic library settings has been slow and inadequate. Most Nigerian university libraries operate without formal data protection compliance frameworks aligned with the NDPA and without cybersecurity governance structures that meet the requirements of modern information security management standards such as ISO/IEC 27001.

The central problem this study addresses is therefore the dangerous mismatch between the growing cybersecurity threat environment confronting Nigerian academic digital libraries, on the one hand, and the institutional, technical, human capital, and policy capacity available to manage those threats effectively, on the other.

1.3 Scope of the Study

This study focuses on cybersecurity and information management in the digital libraries of Nigerian academic institutions, with primary attention to federal and state universities. The temporal scope encompasses the period from 2019 when the NDPR established Nigeria's first comprehensive data protection regulatory framework to 2025, during which period the most significant developments in both the cyberthreat landscape and the national policy

framework have occurred. The study gives particular attention to developments from 2023 onwards, including the British Library ransomware attack (2023), the NDPA (2023), the amended Cybercrimes Act (2024), and recent empirical studies of cybersecurity conditions in Nigerian university libraries.

Thematically, the study covers five domains: (i) the nature and typology of cyberthreats confronting Nigerian academic digital libraries; (ii) information management practices and their cybersecurity dimensions; (iii) the national policy and regulatory framework for cybersecurity and data protection in academic settings; (iv) institutional strengths and weaknesses in cybersecurity governance; and (v) emerging technologies and future directions for digital library security. The study does not undertake primary field surveys but synthesises findings from existing empirical studies, policy documents, and theoretical frameworks to produce an integrated analytical account.

1.4 Significance of the Study

This study makes several significant contributions at multiple levels.

Academically, the study advances the body of scholarship on cybersecurity and information management in library and information science, particularly in the African and specifically Nigerian context. While international scholarship on library cybersecurity is growing rapidly (Oladokun et al., 2024; Corrado, 2024; Akor et al., 2024), Nigerian-focused, comprehensive, and contemporary analytical studies that integrate the policy, institutional, technical, and human dimensions of academic library cybersecurity remain comparatively scarce. This study fills that gap by providing an integrated, theoretically grounded, and empirically anchored analysis.

For library administrators and university management, the study provides a structured diagnosis of the cybersecurity vulnerabilities that place their institutions at risk, alongside actionable recommendations for governance reform. For Nigeria's regulatory and policy community, including NITDA, the Nigeria Data Protection Commission (NDPC), the National Universities Commission (NUC), and the federal Ministry of Education, the study provides evidence for the gaps between national policy intention and institutional implementation and for the targeted regulatory and capacity support that academic institutions require to meet their data protection obligations under the NDPA.

For students, faculty, and library users whose personal and research data are stored in university library systems, the study contributes to awareness of the risks to which their data is exposed and the importance of institutional cybersecurity governance. For funding

agencies and development partners, the study provides an evidence base for targeted investment in cybersecurity capacity building for Nigerian academic institutions.

1.5 Objectives of the Study

This study is designed to achieve the following specific objectives:

i. To identify and analyse the nature, typology, and severity of cybersecurity threats confronting digital libraries in Nigerian academic institutions.
ii. To examine the strengths and weaknesses of current information management practices and cybersecurity governance frameworks in Nigerian university libraries.
iii. To assess the adequacy and implementation effectiveness of Nigeria's national cybersecurity and data protection policy framework as it applies to academic digital library settings.

1.6 Research Questions

This study is guided by the following research questions:

i. What is the nature, typology, and relative severity of cybersecurity threats facing digital libraries in Nigerian academic institutions?
ii. What are the principal strengths and weaknesses of current cybersecurity and information management practices in Nigerian university libraries?
iii. To what extent does Nigeria's national cybersecurity and data protection policy framework adequately address the specific needs and vulnerabilities of academic digital library settings?

2. Review of Related Literature

2.1 Digital Libraries in Nigerian Academic Institutions: Evolution and Context

The evolution of digital libraries in Nigerian universities has been shaped by the intersection of technological advancement, national education policy, and the global open access movement. From the late 1990s onwards, Nigerian universities began acquiring electronic databases, establishing internet connectivity, and developing digital cataloguing systems. The establishment of the Nigerian Research and Education Network (NgREN) and the Virtual Library for Nigeria, supported by UNESCO and other international partners, accelerated the availability of digital academic resources across Nigerian institutions from the mid-2000s (Ezema and Eze, 2024).

By the 2020s, most federal universities and many state universities in Nigeria had established functional digital library platforms, online public access catalogues, and institutional repositories digital archives of the research outputs of their academic communities. These repositories, when well-maintained, represent significant intellectual property assets and contain sensitive data including patron personal information, unpublished research, and confidential academic records. However, surveys consistently document significant variations in the quality, resourcing, and security of digital library systems across Nigerian universities, with federal institutions generally better resourced than their state counterparts (Njoku et al., 2023).

2.1.1 The Cybersecurity Threat Landscape in Nigerian Academic Digital Libraries

Empirical studies of cyberthreats in Nigerian university libraries have mapped a consistent and concerning threat landscape. Obim and Akpokurerie (2023), in a survey of university libraries in South-East Nigeria, identified computer viruses as the most prevalent cybersecurity threat (mean score 3.21), followed by hacking (2.98), unauthorised access to information resources (2.98), password sniffing (2.76), and impersonation (2.68). Ransomware attacks, website spoofing, cyberextortion, and denial of service attacks were also documented, though at lower mean severity scores. These findings align with those of Ibraheem et al. (2025), whose survey of digital library professionals in Kwara State found that data breaches, ransomware, and phishing were the threats perceived as most disruptive to library operations.

Oladokun et al. (2024), in a study of cybersecurity risks in African university libraries, including Nigerian institutions, found that academic libraries face threats encompassing line tapping, improper system processing, and the deployment of malicious software threats that carry the potential for loss of sensitive data, reputational damage, and financial losses. The study noted that the shared-access nature of library computing environments where multiple users access systems through shared terminals, open Wi-Fi, and unsecured network connections creates particular vulnerabilities to social engineering attacks and credential theft (Cybersecurity Risk Modelling, 2025).

The broader Nigerian cybersecurity environment provides important context for understanding library-specific risks. Analysis of cybersecurity incidents across Nigerian institutional settings indicates that ransomware incidents rose by 287 per cent and phishing attempts by 178 per cent between 2020 and 2024 (IJRISS, 2025). The Nigeria Cyber Security Report (2023) documented a 40 per cent increase in reported cybercrime incidents between 2020 and 2023. This deteriorating national threat environment has direct

implications for academic institutions, whose networks, systems, and data repositories are increasingly targeted as accessible points of entry into the broader national information infrastructure.

The British Library ransomware attack of October 2023, which disrupted services for months, compromised significant volumes of patron and staff data, and cost millions of pounds to remediate, served as a global wake-up call for information institutions about the catastrophic potential of sophisticated cyberattacks (Igbinovia & Ishola, 2023). Nigerian library administrators and information professionals cited this incident as a harbinger of risks that their own institutions were ill-prepared to face.

2.1.2 Information Management Challenges in Nigerian Academic Digital Libraries

Beyond cybersecurity threats per se, the broader information management environment of Nigerian academic digital libraries presents challenges that directly shape cybersecurity vulnerability. Ezema and Eze (2024) identify four categories of challenges that hinder effective security: inadequate policies, insufficient ICT skills, power supply issues, and institutional resistance to change. IIARD (2025), in a comprehensive review of security challenges in Nigerian academic library management, found that most institutions rely on "traditional security measures with limited technological intervention", leaving them vulnerable to both physical and cyber threats.

Funding constraints constitute one of the most consistent and significant challenges. Nigerian university libraries are chronically underfunded relative to their operational needs, and cybersecurity, perceived as a specialist, high-cost investment, tends to receive low priority in budget allocation decisions. This results in outdated hardware and software, failure to procure and maintain licensed security software, inability to employ dedicated IT security personnel, and inability to provide regular cybersecurity training to library staff (Nakiyingi, 2024).

Human capital deficits compound funding constraints. Igbinovia and Ishola (2023) found that most Nigerian university librarians possess basic knowledge of cybercrime categories but lack the deeper technical understanding of cybersecurity threats and defences needed to protect digital library environments effectively. Library and information science curricula at Nigerian universities have been slow to integrate cybersecurity as a substantive component of professional training, a gap that has produced a generation of library professionals ill-equipped to manage the security dimensions of their increasingly digital operational environment (Igbinovia & Ishola, 2023; Akor et al., 2024).

The infrastructural environment also poses distinct challenges. Nigeria's unreliable electricity supply, with average grid availability well below 50 per cent of required capacity in many university environments (NBS, 2024), creates conditions under which continuous monitoring of information systems, regular software updates, and consistent implementation of security protocols are practically difficult. Power fluctuations and outages increase hardware vulnerability, disrupt security monitoring tools, and create windows of system vulnerability that can be exploited by cybercriminals.

2.1.3 The National Policy and Regulatory Framework

Nigeria's national framework for cybersecurity and data protection has undergone significant development over the period covered by this study. The foundational instrument remains the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015, which criminalises a range of cyber offences, including hacking, identity theft, and unauthorised system access, and imposes obligations on service providers regarding data retention and support for law enforcement (Digital Policy Alert, 2025). The Act assigns enforcement responsibilities to multiple agencies, including the Nigerian Police Force, the Economic and Financial Crimes Commission (EFCC), and the Office of the National Security Adviser (ONSA).

A significant development came in February 2024 when the National Assembly amended the Cybercrimes Act, introducing a 72-hour mandatory incident reporting requirement for cyberattacks on regulated entities, expanding definitions of cybercrime, strengthening identity verification requirements, and enhancing international cooperation mechanisms (Digital Policy Alert, 2025). The same period saw the president sign an executive order in June 2024 designating specific computer systems, networks, and communication infrastructure as critical national infrastructure, subjecting them to enhanced oversight by the ONSA.

On the data protection front, the NDPR of 2019, Nigeria's first comprehensive data protection regulation, issued by NITDA, established principles for the collection, processing, and storage of personal data applicable to all data controllers, including academic institutions (NITDA, 2020). The NDPR was superseded by the Nigeria Data Protection Act (NDPA) of 2023, which established the Nigeria Data Protection Commission (NDPC) as an independent statutory body, set binding obligations for data controllers and processors, and aligned Nigeria's data protection framework more closely with international standards, including the EU General Data Protection Regulation (GDPR). As of 19 September 2025, the General Application Implementation Directive

(GAID) issued by the NDPC has replaced the NDPR as the primary implementing instrument under the NDPA (ICLG, 2025).

University libraries, as processors of significant volumes of patron personal data, including identity information, borrowing records, research profiles, and digital access logs, are unambiguously subject to the obligations of the NDPA. These obligations include the appointment of a data protection officer, the conduct of data protection impact assessments (DPIAs) for high-risk processing activities, the implementation of appropriate technical and organisational security measures, and mandatory reporting of data breaches to the NDPC. However, empirical evidence suggests that most Nigerian university libraries have not yet achieved compliance with these obligations, and the NDPC has not yet developed sector-specific guidance for academic library compliance (Farid & Hassan, 2023; IIARD, 2025).

2.1.4 Existing Cybersecurity Strengths and Good Practices

While the challenges are substantial, research also documents areas of strength and emerging good practice. Ibraheem et al. (2025) found that academic libraries in Nigeria, while generally lagging public libraries in data encryption practices, demonstrate comparatively stronger performance in access control mechanisms and regular software update practices, security measures that are foundational to basic system protection. Surveys of library professionals in some Nigerian universities document growing awareness of cybersecurity risks and increasing demand for training and capacity development.

Several Nigerian universities have invested in institutional repository management systems with built-in security features, including encrypted connection protocols, role-based access control, and automated backup systems (Njoku et al., 2023). The NUC's accreditation requirements for university libraries include basic ICT infrastructure standards that create a minimum floor for digital library development, and some universities have begun developing library-specific information security policies in response to growing awareness of cybersecurity risks (African Journal of Library, Archives and Information Science, 2025).

At the national level, NITDA's capacity-building programmes, including the 3 Million Technical Talent (3MTT) initiative launched in 2023, have the potential to increase the supply of ICT professionals in Nigeria, some of whom may serve in academic library settings. The NDPA's establishment of the NDPC as an independent regulator provides a

more credible and empowered institutional framework for data protection enforcement than the previous NITDA-administered NDPR regime (Lexology, 2023).

2.2 Theoretical Framework

This study is anchored in two complementary theoretical frameworks that together provide a comprehensive analytical architecture for examining cybersecurity and information management in Nigerian academic digital libraries.

2.2.1 The CIA Triad Model

The CIA Triad such as Confidentiality, Integrity, and Availability, is the foundational conceptual framework of information security and constitutes the standard against which cybersecurity governance in any information system, including digital libraries, is evaluated. Confidentiality refers to ensuring that information is accessible only to those authorised to access it, preventing unauthorised disclosure of patron data, research outputs, and institutional records. 'Integrity' refers to the accuracy and completeness of information, ensuring that library data is not altered, corrupted, or deleted through unauthorised means. 'Availability' refers to the reliable accessibility of information systems and resources to authorised users, ensuring that cyberthreats do not disrupt library service delivery.

Applied to the Nigerian academic digital library context, the CIA Triad provides a structured framework for assessing the specific ways in which identified cyberthreats compromise each dimension of security. Ransomware attacks primarily threaten availability; data breaches primarily threaten confidentiality; malware infections that corrupt data files primarily threaten integrity. A comprehensive cybersecurity governance framework must address all three dimensions simultaneously, a requirement that most Nigerian university libraries currently fail to meet (Njoku et al., 2023; Obim & Akpokurerie, 2023).

2.2.2 Information Security Management Systems (ISMS) Theory

ISMS theory, formalised in the ISO/IEC 27001 international standard, provides a systematic framework for establishing, implementing, maintaining, and continuously improving an organisation's information security management. The ISMS model holds that effective information security cannot be achieved through ad hoc or purely technical measures but requires a systematic, risk-based, and continuously improving management system that integrates technical controls, organisational policies, human resource

management, physical security, and compliance management into a coherent governance framework.

The ISMS framework is directly applicable to the governance challenge facing Nigerian academic digital libraries. The consistent finding in empirical research that most Nigerian university libraries lack formal information security policies, dedicated security personnel, documented risk assessments, and structured incident response protocols reflects the absence of an ISMS-based approach to security governance. Adopting ISO/IEC 27001 or an equivalent framework adapted to the Nigerian academic context would provide institutions with a structured path toward systematic security improvement (Aregbesola & Nwaolise, 2023).

3 Methodology

3.1 Research Design

This study employs a qualitative descriptive research design, involving the systematic collection, critical analysis, and interpretive synthesis of secondary data sources relevant to the study's research questions. A qualitative design is appropriate for this study because the central analytical challenges understanding the nature of cyberthreats, assessing the adequacy of governance frameworks, evaluating institutional strengths and weaknesses, and formulating policy recommendations require interpretive analysis of institutional contexts and policy processes rather than purely statistical measurement. Black and Champion (1976) affirm that qualitative designs are best suited to studies seeking to explain complex social and institutional phenomena in their context, rather than merely measuring their frequency.

3.2 Data Collection Strategy

Data were collected through systematic secondary research, encompassing four categories of sources: (i) peer-reviewed academic journal articles and conference papers published between 2019 and 2025, sourced from databases including Google Scholar, ResearchGate, Wiley Online Library, Emerald Insight, and African Journals Online (AJOL); (ii) policy documents and regulatory instruments including the NDPR (2019), the NDPA (2023), the Cybercrimes Act (2015, as amended 2024), NITDA guidelines, and the NUC's library accreditation standards; (iii) reports from international and national organisations including the Nigerian Cyber Security Report (2023), the NDPC, NITDA, and relevant ICLG guidance; and (iv) authoritative professional and institutional assessments including the

FUDMA Journal of Sciences' 2025 study of Kwara State digital libraries, the IIARD (2025) review, and relevant African Journal of Library, Archives and Information Science publications. All sources were evaluated for credibility, methodological rigour, and relevance before incorporation.

3.3 Data Analysis

Data were analysed using thematic analysis, a method involving the systematic identification, coding, and organisation of recurring patterns and themes across collected materials. Thematic analysis was conducted in five stages: familiarisation with the data through comprehensive reading; generation of initial codes from the data; clustering of codes into broader themes aligned with the study's research questions and theoretical frameworks; reviewing and refining themes against the full dataset; and producing the analytical narrative. Content analysis was also applied to policy documents, enabling systematic assessment of the coverage, gaps, and implementation provisions of the national regulatory framework as it applies to academic digital library settings.

4. Major Findings

4.1 Finding 1: A Multi-Dimensional and Escalating Threat Landscape

Nigerian academic digital libraries face a multi-dimensional cyberthreat landscape whose severity is increasing. The most prevalent documented threats are computer viruses, hacking, and unauthorised access to information systems, followed by password sniffing, impersonation, phishing, ransomware, social engineering, insider threats, and denial of service attacks (Obim & Akpokurerie, 2023; Ibraheem et al., 2025). These threats are not static: ransomware incidents in Nigerian institutional settings rose by 287 per cent between 2020 and 2024, and phishing attempts increased by 178 per cent in the same period (IJRISS, 2025). The shared-access computing environments characteristic of academic libraries, with multiple users accessing systems through shared terminals and open network connections, create particular vulnerability to credential theft and social engineering.

4.2 Finding 2: Critical Weaknesses in Institutional Cybersecurity Governance

The dominant institutional condition characterising Nigerian academic digital libraries is the absence of systematic cybersecurity governance. Most Nigerian university libraries operate without formally documented information security policies, without dedicated cybersecurity personnel, without regular risk assessments, and without structured incident

response protocols (Ezema & Eze, 2024; IIARD, 2025). The vast majority of institutions have not conducted data protection impact assessments as required by the NDPA, have not appointed data protection officers as mandated, and do not have library-specific data breach notification procedures. This governance vacuum means that even when technical security measures exist, they are not deployed within a coherent framework that ensures their consistent and effective implementation.

4.3 Finding 3: Acute Human Capital Deficits

A severe shortage of cybersecurity-trained library and information science professionals constitutes one of the most critical vulnerabilities in Nigerian academic digital library security. Igbinovia &Ishola (2023) found that most Nigerian university librarians have only basic awareness of cybercrime categories and lack the deeper technical and governance knowledge needed to manage digital library security effectively. Library and information science education programmes in Nigeria have been slow to integrate cybersecurity competencies into their curricula, producing graduates insufficiently prepared for the security management demands of contemporary digital library environments (Akor et al., 2024). This human capital deficit is particularly acute in state university libraries, where recruitment of specialist ICT personnel competes with severe funding constraints.

4.4 Finding 4: Infrastructure and Resource Constraints

Structural infrastructure deficits significantly amplify cybersecurity vulnerabilities in Nigerian academic digital libraries. Chronic underfunding results in outdated hardware, unlicensed or outdated security software, an absence of redundant backup systems, and an inability to procure and maintain intrusion detection and prevention systems. Nigeria's unreliable electricity supply disrupts continuous system monitoring, prevents timely software updates, and creates hardware vulnerabilities through irregular power fluctuations and outages. These constraints are particularly acute in state universities and in institutions located outside major urban centres, where both funding and ICT infrastructure quality are typically lower than in federal institutions.

4.5 Finding 6: Emerging Strengths and Best-Practice Islands

Research also documents emerging strengths and pockets of good practice. Some Nigerian university libraries have implemented role-based access control systems, encrypted connection protocols, and automated backup procedures for institutional repositories. Academic libraries generally demonstrate stronger access control practices than public

libraries (Ibraheem et al., 2025). Growing professional awareness of cybersecurity risks stimulated by international incidents such as the British Library ransomware attack and by national capacity-building initiatives is driving increasing demand for cybersecurity training among library professionals. The NUC's accreditation standards create a minimum floor for ICT infrastructure in university libraries. The national 3MTT initiative is increasing the supply of ICT professionals from whom academic institutions may draw cybersecurity expertise.

5. Discussion of Findings

The findings of this study converge on a central conclusion. Nigerian academic digital libraries face a growing and genuinely dangerous cybersecurity challenge that their current institutional governance, human capital, technical infrastructure, and policy implementation capacity are substantially inadequate to address. This conclusion is not a counsel of despair; the study also identifies real strengths, improving trends, and a progressively strengthening national policy framework, but it does require honest acknowledgement of the gap between aspiration and current reality.

The CIA Triad framework reveals that all three dimensions of information security confidentiality, integrity, and availability are meaningfully compromised in the typical Nigerian academic digital library. Patron personal data is inadequately protected by confidentiality controls; library records and digital collections are vulnerable to integrity-compromising malware and unauthorised access; and the reliance on unreliable electrical infrastructure, combined with the absence of robust backup and recovery systems, creates chronic availability risks. Meeting the CIA standard requires a comprehensive, simultaneous improvement across all three dimensions, a requirement that demands substantially greater investment and governance commitment than most Nigerian university libraries currently receive.

The ISMS framework illuminates why the dominant pattern of ad hoc and technically fragmented security measures has produced such poor outcomes. Security measures that are not integrated within a coherent management system such as one that includes formal policy, assigned responsibilities, risk assessment, performance monitoring, and continuous improvement, will inevitably have gaps that determined attackers will exploit. The ISO/IEC 27001 framework or its equivalent provides a proven pathway to systematic security governance that Nigerian academic libraries should be supported and required to adopt.

Routine Activity Theory directs attention to the practical strategic priority: since the supply of motivated offenders in Nigeria's cybercrime environment cannot be effectively controlled by academic institutions, the most productive investments are in target hardening (making library systems more technically difficult to attack) and in strengthening capable guardianship (investing in trained, vigilant, and empowered security personnel). Both require financial investment that most Nigerian university libraries currently lack, pointing to the need for institutional budget reform, NUC accreditation standard revision, and potentially dedicated federal support for cybersecurity capacity in academic institutions.

The socio-technical systems lens is perhaps the most practically instructive. The empirical evidence consistently shows a damaging mismatch between the technical security controls that exist (access controls, software updates, basic firewalls) and the social conditions required to make them effective (trained staff, institutional policies, governance accountability, and security culture). Closing this mismatch requires not only technical investments, but also simultaneous investments in professional training, curriculum reform in LIS education, institutional policy development, and the cultivation of a security-conscious organisational culture across Nigerian academic library institutions. The policy analysis findings raise an important governance concern. Nigeria has invested significant effort in constructing an increasingly robust national cybersecurity and data protection policy framework, culminating in the NDPA of 2023 and the amended Cybercrimes Act of 2024, but the translation of this framework into effective institutional practice in academic library settings has been left largely to individual institutions without the sector-specific guidance, enforcement pressure, or capacity support that would be needed to drive systematic compliance. The NDPC, the NUC, and university management must together close this translation gap.

5.1 Summary

This study has examined cybersecurity and information management in digital libraries of Nigerian academic institutions, with specific focus on the emerging challenges, policy framework, institutional capacities, and strategic directions for improvement. Drawing on a systematic review of contemporary empirical research, policy documents, and theoretical frameworks, the study identified six major findings.

Nigerian academic digital libraries face a multi-dimensional and escalating cyberthreat landscape encompassing viruses, hacking, phishing, ransomware, unauthorised access, and insider threats. Institutional cybersecurity governance is characterised by

critical weaknesses: absence of formal security policies, lack of dedicated security personnel, non-compliance with NDPA obligations, and inadequate incident response frameworks. Human capital deficits, particularly the insufficient integration of cybersecurity competencies in library and information science education, represent a structural vulnerability. Infrastructure and funding constraints amplify technical vulnerabilities. Nigeria's national policy framework has been substantially strengthened through the NDPA (2023) and the amended Cybercrimes Act (2024), but implementation in academic library settings remains incomplete. Some islands of best practice exist, and professional awareness is growing.

Four theoretical frameworks such as the CIA Triad, ISMS Theory, Routine Activity Theory, and Socio-Technical Systems Theory, together provide an integrated analytical architecture for understanding these findings and for designing effective responses. The study advances seven specific policy recommendations.

5.2 Conclusion

The digital transformation of Nigerian academic libraries represents a genuine developmental achievement, one that has expanded access to knowledge, strengthened research capacity, and connected Nigerian scholars to global information networks. But this transformation has also created a complex and growing set of cybersecurity vulnerabilities that the sector has not yet equipped itself to manage effectively.

The threat landscape is real, sophisticated, and escalating. The institutional governance frameworks are inadequate. The human capital is insufficient. The infrastructure is fragile. Moreover, the translation of a progressively strengthened national policy framework into effective institutional practice has been slow and uneven. The British Library's 2023 ransomware catastrophe is a reminder that even well-resourced institutions with trained staff and sophisticated systems can be devastated by a successful cyberattack. Nigerian academic digital libraries, operating with far fewer resources and in a far more challenging security environment, are at even greater risk.

Addressing this challenge requires a sustained, multi-stakeholder, and multi-level response: reform of LIS education curricula; development of NDPA-compliant institutional security policies; investment in technical infrastructure; capacity building for library professionals; sector-specific regulatory guidance from the NDPC and NUC; and a governance culture that treats cybersecurity not as a technical add-on but as a core institutional responsibility. The digital future of Nigerian academic libraries depends on getting this right.

5.3 Policy Recommendations

5.3.1 Mandate Institution-Specific Information Security Policies

The National Universities Commission (NUC) should revise its library accreditation standards to require all universities to develop, implement, and annually review a formal information security policy for their digital libraries. This policy must document threat risk assessments, access control frameworks, incident response procedures, data breach notification processes, staff responsibility assignments, and performance monitoring mechanisms. The NUC should provide a model policy template aligned with NDPA obligations and ISO/IEC 27001 principles to support institutions in policy development.

5.3.2 Integrate Cybersecurity into Library and Information Science Education

Nigerian universities offering Library and Information Science programmes should revise their curricula to include substantive coverage of cybersecurity theory and practice; data protection law and compliance; digital preservation security; information risk management; and incident response. Professional bodies including the Nigerian Library Association (NLA) and the Librarians' Registration Council of Nigeria (LRCN) should develop mandatory continuing professional development programmes in cybersecurity for practising library professionals. Partnerships with computer science and cybersecurity faculties should be formalised to enable cross-disciplinary training.

5.3.3 Establish a Dedicated National Funding Stream for Academic Library Cybersecurity

The Federal Ministry of Education, the Tertiary Education Trust Fund (TETFund), and the NUC should establish a dedicated annual funding stream specifically for cybersecurity infrastructure investment in university library systems. This fund should support the procurement of licensed security software, installation of intrusion detection systems, implementation of encrypted network protocols, development of off-site backup and recovery systems, and appointment of dedicated library ICT security personnel. Applications for this fund should require institutions to demonstrate a compliant information security policy as a condition of eligibility.

5.3.4 Issue Sector-Specific NDPA Compliance Guidance for Academic Libraries

The Nigeria Data Protection Commission (NDPC) should issue sector-specific guidance for academic libraries addressing their specific data protection obligations under the NDPA

of 2023. This guidance should address the appointment of data protection officers in library settings; the conduct of data protection impact assessments for high-risk library processing activities (particularly patron borrowing records and digital access logs); specific data breach notification procedures; requirements for privacy notices to library users; and guidance on data retention and deletion schedules for personal data. The NDPC should develop a simplified compliance framework for academic libraries that reduces compliance costs while maintaining substantive data protection standards.

5.3.5 Develop Collaborative Cybersecurity Networks among Nigerian Universities

The Nigerian university sector should establish a University Libraries Cybersecurity Consortium, a collaborative network that enables academic libraries to share threat intelligence, incident reports, security solutions, staff training resources, and cybersecurity expertise. Such a consortium could pool resources for collaborative procurement of security software, joint training programmes, shared threat monitoring services, and collective responses to sector-wide cybersecurity incidents. Models from comparable collaborative security networks in the United Kingdom (JISC) and the United States (EDUCAUSE) provide proven templates for such a consortium.

5.3.6 Implement Mandatory Cybersecurity Awareness Training

University library management should implement mandatory, regular cybersecurity awareness training for all library staff, not only ICT specialists but all personnel who access library information systems. This training should cover recognition and reporting of phishing attempts, safe password management practices, procedures for handling suspicious system behaviour, responsibilities under the NDPA, and the institution's incident response protocols. Training should be updated at least annually to reflect the evolving threat landscape, and compliance with training requirements should be tracked and enforced as a condition of system access.

5.3.7 Invest in Resilient Infrastructure and Backup Systems

Nigerian universities should prioritise investment in the electrical and network infrastructure that underpins digital library security. This includes: installation of Uninterruptible Power Supply (UPS) systems and solar backup power for critical library servers and monitoring systems; migration of key library systems to cloud-based platforms with built-in redundancy and security; implementation of automated, off-site data backup systems with tested recovery procedures; and upgrading of network infrastructure to

support encrypted connections for all digital library access. Government infrastructure initiatives, including the proposed national fibre optic rollout and university campus power upgrade programmes, should explicitly include digital library systems in their scope.

References

Akor, A., Nongo, C., Udofot, C., & Oladokun, B. D. (2024). Cybersecurity awareness: Leveraging emerging technologies in the security and management of libraries in higher education institutions. *Southern African Journal of Security.* https://doi.org/10.25159/3005-4222/16671

Aregbesola, A., & Nwaolise, E. L. (2023). Securing digital collections: Cyber security best practices for academic libraries in developing countries. *Library Philosophy and Practice*, 7822. https://digitalcommons.unl.edu/libphilprac/7822

Black, J. A., & Champion, D. J. (1976). Methods and issues in social research. John Wiley & Sons.

British Library. (2024). British Library cyber incident: Review and lessons learned. British Library.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: *A routine activity approach. American Sociological Review, 44(4), 588–608.*

Corrado, E. M. (2024). Cybersecurity in academic libraries: Emerging threats and institutional responses. Journal of Library Administration.

Cybersecurity Risk Modeling in Library Information Systems. (2025). *International Journal of Information Security and Safety Research* (IJISS). https://ojs.trp.org.in/index.php/ijiss/article/download/5421/7963

Digital Policy Alert. (2025). DPA digital digest: Nigeria 2025 edition. Digital Policy Alert. https://digitalpolicyalert.org/digest/dpa-digital-digest-nigeria

Emery, F. E., & Trist, E. L. (1960). Socio-technical systems. In C. W. Churchman & M. Verhulst (Eds.), *Management science: Models and techniques* (Vol. 2, pp. 83–97). Pergamon.

Ezema, I. J., & Eze, B. (2024). Status and challenges of institutional repositories in university libraries in South-East Nigeria: Implications for visibility and ranking of Nigerian universities. *The Journal of Academic Librarianship, 50(2), 102834.*

Farid, G., & Hassan, S. (2023). Digital information security management policy in academic libraries: A systematic review and implementation study. *Journal of Academic Librarianship, 49(2), 102634.*

Federal Republic of Nigeria. (2015). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. Federal Government of Nigeria.

Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023. Federal Government of Nigeria.

Federal Republic of Nigeria. (2024, February). Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Amendment Act, 2024). Federal Government of Nigeria.

ICLG (International Comparative Legal Guides). (2025). Data protection laws and regulations 2025–2026: Nigeria. ICLG. https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria/

Ibraheem, I., Yusuf, A. A., Aremu, B. L., & Jidda, M. T. (2025). Perspectives of librarians on the impact of cyber threats in the management of digital libraries in Kwara State, Nigeria. *FUDMA Journal of Sciences*, 9(12), 9–19. https://fjs.fudutsinma.edu.ng/index.php/fjs/article/view/3990

Igbinovia, M. O., & Ishola, B. C. (2023). Cyber security in university libraries and implication for library and information science education in Nigeria. *Digital Library Perspectives*, 39(3), 248–266. https://doi.org/10.1108/DLP-11-2022-0089

IIARD (International Institute of Academic Research and Development). (2025). Enhancing the security of information in academic libraries: Challenges and strategies for sustainable management. *Research Journal of Management and Computer and Information Technology (RJMCIT), 11(7), 213–230.*

International Journal of Research and Innovation in Social Science (IJRISS). (2025). Analysis of emerging cybersecurity threats in Nigeria's financial institutions. *IJRISS*, 9(7). https://rsisinternational.org/journals/ijriss

ISO/IEC 27001:2022. (2022). Information security, cybersecurity and privacy protection — Information security management systems, Requirements. *International Organization for Standardization.*

Lexology. (2023). In a nutshell: Data protection, privacy and cybersecurity in Nigeria. Lexology. https://www.lexology.com/library/detail.aspx?g=f44586b1-0048-4d93-a461-4d8c0aada232

Nakiyingi, R. L. (2024). Strengthening cybersecurity in Nigerian libraries: Challenges, mitigation strategies, and future trends. *Research Output Journal of Biological and Applied Science*, 3(2), 23–27. https://www.researchgate.net/publication/383875848

National Bureau of Statistics (NBS). (2024). Nigeria electricity report 2023–2024. NBS.

National Information Technology Development Agency (NITDA). (2019). Nigeria Data Protection Regulation (NDPR). NITDA.

National Information Technology Development Agency (NITDA). (2020). NDPR implementation framework. NITDA. https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf

National Universities Commission (NUC). (2024). List of accredited universities in Nigeria. NUC.

Nigerian Cyber Security Report. (2023). Annual cybersecurity threat landscape: Nigeria 2023. Nigeria Cybercrime Advisory Council.

Njoku, I. S., Njoku, B. C., Chukwu, S. A. J., Eke, F. M., & Haco-Obasi, F. C. (2023). Fostering cybersecurity in institutional repositories: A case of Nigerian universities. *African Journal of Library, Archives and Information Science, 33(1).*

Nnenda, W., & Aforomo, T. M. (2023). Information resources and security challenges in Niger Delta University, Bayelsa State, Nigeria. Library Philosophy and Practice.

Obim, I. E., & Akpokurerie, A. O. (2023). Awareness of cybersecurity and its impact on information storage in the university libraries in South East Nigeria. 3(2).

Oladokun, B., Oloniruha, E., Mazah, D., & Okechukwu, O. (2024). Cybersecurity risks: A sine qua non for university libraries in Africa. *Southern African Journal of Security,* 2, 14 pages. https://doi.org/10.25159/3005-4222/15320

Olumide, O., & Adejumo, G. (2022). Future trends in library cybersecurity: The potential of AI and blockchain in Nigerian libraries. *Journal of Library and Information Technology, 42(2), 89–102.*

Pasqui, V. (2024). Digital curation and long-term digital preservation in libraries. *JLIS.It,* 15(1), 109–125. https://doi.org/10.36253/jlis.it-567

University of Jos. (2024). Digital economy and Nigeria's national security. *Unijos Journal of Political Science, Special Edition*. https://journals.unijos.edu.ng/index.php/ujjps/article/download/779/394

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. *European Journal of Criminology, 2(4), 407–427.*

Zhang, L., et al. (2025). Unsecured APIs and authentication vulnerabilities in academic information systems. Journal of Information Security, 16(2).