
CYBERSECURITY GOVERNANCE, DIGITAL RESILIENCE AND CONTINUITY OF ELECTRONIC LIBRARY SERVICES IN UNIVERSITY LIBRARIES IN SOUTH-SOUTH NIGERIA: DEVELOPING AN INSTITUTIONAL CYBER-RESILIENCE FRAMEWORK

 Aba, Jane Igie^{1*},  Omwanghe Etinosa James²,  Omoregie Godsent Osagie³ &  Ogueri Abel Obaro⁴

¹Department of Library & Information Science, Faculty of Social Sciences, Ambrose Alli University, Ekpoma, Edo State, Nigeria

^{2,3,4}John Harris Library, University of Benin, Edo State, Nigeria

<http://doi.org/10.35409/IJBMER.2026.3806>

Received: 15 July 2026/ Published: 28 August 2026

ABSTRACT

The rapid digitization of university library services has increased institutional dependence on electronic journals, databases, e-books, repositories and cloud-based platforms, while simultaneously exposing these services to growing cybersecurity risks. This study examines cybersecurity governance, digital resilience and continuity of electronic library services in university libraries in South-South Nigeria, with specific purpose of developing and validating a context-specific institutional cyber-resilience framework. A mixed-methods research design was adopted across 10 universities comprising six Federal, two State and two Private institutions. Data was obtained from 161 valid respondents, representing an 80.5% response rate and analyzed using descriptive statistics, Pearson correlation, multiple regression and expert validation. Findings revealed moderate levels of cybersecurity governance ($\bar{x} = 3.18$), human capacity ($\bar{x} = 3.05$), technology and infrastructure ($\bar{x} = 3.27$), response and recovery capacity ($\bar{x} = 2.91$), digital resilience ($\bar{x} = 3.12$) and continuity of electronic library services ($\bar{x} = 3.24$). Significant positive relationships exist among study variables, with digital resilience strongly associated with service continuity ($r = .81$, $p < .01$). The regression model had 68% of the variance in digital resilience, with response and recovery capacity making the strongest contribution ($\beta = .34$), followed by technology and infrastructure ($\beta = .29$), cybersecurity governance ($\beta = .23$) and human capacity ($\beta = .19$). Digital resilience significantly predicted continuity of electronic library services ($\beta = .81$, $R^2 = .66$, $p < .001$). Expert validation produced an overall mean of 4.48, confirming the framework's relevance and applicability. The study contributes an institutionally grounded cyber-resilience framework that integrates governance, human capacity, technology, response, recovery to strengthen sustainable electronic library services and inform university management, TETFund and regulatory policy.

Keywords: Cybersecurity governance; Digital resilience; Electronic library services; Cyber-resilience framework; University libraries; South-South Nigeria.

1. INTRODUCTION

Background and Context

Currently, rapid digitization of university library services has transformed access to scholarly information. Electronic journals, databases, e-books, institutional repositories and cloud-based platforms to form an integral part of teaching, learning and research. However, digital dependence also increases exposure of library systems to malware, phishing, password attacks, unauthorized access, data breaches and service disruption. Studies from Nigerian university libraries indicate that technological expansion is accompanied by cybersecurity issues and inadequate cybersecurity knowledge among library personnel (Igbिनovia & Ishola, 2023). These challenges extend beyond protecting computers and networks. Electronic library services depend on interaction of technology, people, institutional policies, funding, skills and operational procedures. Therefore, vulnerability in any of these elements can compromise access to scholarly resources, notwithstanding the presence of basic technical controls. Similarly, African research identifies cybersecurity as an emerging concern for university libraries with potential consequences for information security, institutional reputation and service delivery (Oladokun et al., 2024). Thus, cybersecurity should be understood not only as a technical function but also as an institutional governance and resilience issue. This perspective is captured in NIST Cybersecurity Framework 2.0, that incorporates Govern with Identify, Protect, Detect, Respond and Recover. The framework recognizes cybersecurity as an organizational risk that requires leadership, policies, responsibilities and continuous risk management rather than isolated technical interventions (Pascoe et al., 2024). This implies that effective cybersecurity should be evaluated by their capacity to maintain reliable electronic services before, during and after security breaches in university libraries.

Problem Statement

Despite growing relevance of electronic resources, cybersecurity research in Nigerian university libraries focused on identifying threats, assessing awareness and examining protective measures, Igbिनovia & Ishola (2023) noted cybersecurity issues in Nigerian university library personnel, while Oladokun et al. (2024) highlighted broader cybersecurity risks confronting African university libraries. These studies provide important evidence of vulnerability, but they do not sufficiently explain how cybersecurity governance, digital resilience and continuity of electronic library services can be integrated in a single institutional framework.

Additionally, existing research revealed vital gap practices. Although, libraries may acquire antivirus software, passwords and firewalls but could remain vulnerable if cybersecurity responsibilities are unclear due to inadequate staff skills, weak incident-response procedures or lack of effective recovery systems that cannot restore services promptly. Likewise, effective cybersecurity requires synchronized governance, protection, detection, response and recovery activities (NIST, 2024). However, there is limited empirical studies on how these principles can be adapted into operational realities of university libraries in South-South Nigeria. Therefore, this study is beyond mere description of cyber threats to examine institutional conditions that support digital resilience and continuity, uses evidence to develop and validate context-specific institutional cyber-resilience framework for sustainable electronic library services.

Objectives of the Study

The study seeks to:

- 1) assess the level of cybersecurity governance and digital resilience in university libraries in South-South Nigeria.
- 2) examine relationship between cybersecurity governance, digital resilience and continuity of electronic library services in South-South Nigeria.
- 3) develop and validate an institutional cyber-resilience framework for sustaining electronic library services in South-South Nigeria.

Research Questions

The following research questions are answered in this study:

- 1) What is the level of cybersecurity governance and digital resilience in university libraries in South-South Nigeria?
- 2) What relationship exists between cybersecurity governance, digital resilience and continuity of electronic university library services in South-South Nigeria?
- 3) What institutional cyber-resilience framework can be developed and validated to support sustainable electronic university library services in South-South Nigeria?

Significance and Contribution of the Study

This study contributes empirically extending beyond identification of cyber threats to evaluate how governance, people, technology and service continuity interact in university libraries. Basically, the contribution is hinged on the development and validation of a context-specific institutional cyber-resilience framework that will guide universities in preventing, detecting, responding to recovering from cyber disruptions. The findings also have policy relevance for university management, library administrators, ICT units and TETFund by providing evidence for targeted investment in cybersecurity infrastructure, staff capacity, risk governance and service-continuity mechanisms. This approach is consistent with the current shift from fragmented cybersecurity controls towards integrated organizational risk management and resilience (NIST, 2024).

2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

Cybersecurity governance refers to institutional structures, policies, responsibilities and processes through which cybersecurity risks are directed, monitored and controlled. Significantly, it has increased electronic journals, databases, repositories and online discovery systems to become an integral component of scholarly communication in university libraries. Cybersecurity is therefore not solely an ICT responsibility; it is also a governance issue because decisions about access control, data protection, staff responsibilities, risk tolerance, incident reporting and service recovery directly affect library operations. The NIST Cybersecurity Framework 2.0 affirms that by introducing “Govern” as a distinct function with Identify, Protect, Detect, Respond and Recover will synchronize technical security with organizational leadership and risk management (Pascoe et al., 2024).

In Nigeria governance dimension is still underdeveloped. Igbinovia & Ishola (2023) found that cybersecurity issues in university libraries were associated with improved librarians' knowledge and preparedness, indicating that technological adoption without corresponding human capacity

can create new vulnerabilities. Similarly, research on Nigerian institutional repositories identified weaknesses that require stronger cybersecurity practices and institutional attention (Njoku et al., 2023). This implies that university libraries can possess security technologies without possessing cybersecurity capability. Furthermore, Governance will enhance mechanism for synchronizing technology, people, policies and resources to facilitate protection and continuity of electronic services in university libraries in South South, Nigeria.

Digital Resilience and Service Continuity

Digital resilience extends cybersecurity beyond prevention. It refers to an organization's ability to anticipate disruption, withstand adverse events, respond effectively, recover critical functions and adapt after an incident. Lee (2025) states that digital resilience could serve as foundation for sustainable library development rather than constituting an extension of digitization efforts. Similarly, scholars in higher education and research organizations categorized digital resilience into various stages such as before, during and after disruption namely preparedness, response, recovery and organizational learning (Mahmood et al., 2024). Resilience is crucial for electronic library services because cybersecurity failure can hinder availability and continuity of scholarly information even when data are not permanently lost. For instance, a ransomware incident can compromise authentication system or network failure that could prevent students and researchers from accessing databases, repositories and digital resources. Thus, service continuity is paramount to cybersecurity governance than a separate library-management issue. Cervone (2006) also identifies disaster recovery and contingency planning as essential components of digital library planning. Hence, the critical issue is whether university libraries can continue delivering essential electronic services while responding and recovering from cyber disruptions.

Cyber Threats in University Libraries

The expansion of digital library infrastructure has increased cyberattack in university libraries. These threats include malware, phishing, ransomware, password attacks, unauthorized access, identity theft, data breaches and other forms of malicious activity. Oladokun et al., (2024) enumerates cyber threats to include malware, phishing, ransomware and identity theft among major cybersecurity risks that affect information integrity, intellectual property, institutional reputation and financial resources in African university libraries. In the same vein, Al-Hikmah et al. (2025) asserted that data breaches, ransomware and phishing pose risks to integrity and accessibility of digital library services. Hence, there is need for continuous cybersecurity training and context-specific security strategies. However, cyber threats should not be exclusively perceived as external technological attacks. Human behaviour, inadequate skills, weak policies, poor security culture and infrastructural limitations can also amplify vulnerabilities. Igbinovia & Ishola (2023) identified the importance of cybersecurity knowledge among library personnel, while Malatji et al. (2019) affirmed that cybersecurity weaknesses emerge when social, technical and environmental dimensions are not properly integrated. This distinction is central to the present study. The existence of cyber threats is not the core culprit of institutional vulnerability rather, it is shaped by how effectively an institution anticipates, governs, detects, responds and recovers from threats. This premise redirects the research focus from a conventional security-control model to institutional cyber-resilience.

Empirical Research Gap

Existing research provides useful findings on the prevalence of cyber threats, cybersecurity awareness and technical vulnerabilities in university and digital libraries. However, three important gaps still need to be addressed that existing literature focuses on types of threats encountered and awareness of library personnel rather than modelling relationships between governance, resilience and continuity. Secondly, most studies tend to examine technological controls, human awareness and institutional policies separately, despite findings that cybersecurity is inherently socio technical. Thirdly, there is scanty empirical work specifically addressing how cybersecurity investment affects continuity of electronic library services.

Furthermore, the geographical gap is not uniform across geopolitical regions because universities differ in infrastructure, funding, institutional governance, ICT capacity and access to technical expertise. The existing literature acknowledges limited understanding of how cybersecurity risks can be effectively mitigated within distinctive institutional environment of university libraries (Oladokun et al., 2024). Consequently, there is a need for context-specific evidence from South-South, Nigeria that integrates cybersecurity governance, digital resilience and service continuity in a single explanatory and operational framework. The present study addresses this gap by moving from “What cyber threats exist?” to a more consequential question: “What institutional capabilities enable university libraries to maintain electronic services despite cyber threats?” This provides the basis for developing and validating an institutional cyber-resilience framework.

Socio-Technical Systems Theory

This study is anchored on Socio-Technical Systems Theory, originally developed by Emery & Trist (1960). The theory focuses on optimizing social and technical systems than isolated systems. This theory relates to electronic library cybersecurity encompassing technologies, employees, organizational processes, institutional policies and environment. Malatji et al. (2019) used this theory to create a cybersecurity framework that harmonizes social, technical and environmental factors. This analysis reveals that focusing on technological controls can create organizational vulnerabilities, while neglecting other areas to create security gaps. Thus, the theory provides a holistic insight of university library cybersecurity than a technology-centric approach. For instance, firewall cannot compensate for poor password practices; staff training cannot compensate for unsupported infrastructure and cybersecurity policy has limited value where responsibilities, funding and incident-response mechanisms are unverified. Consequently, cyber-resilience emerges from a symbiotic relationship between people, technology, organizational governance and environmental conditions.

This study conceptualizes institutional cyber-resilience as an integrated system comprising four interconnected dimensions as depicted in the diagram below using Socio-Technical Systems Theory.

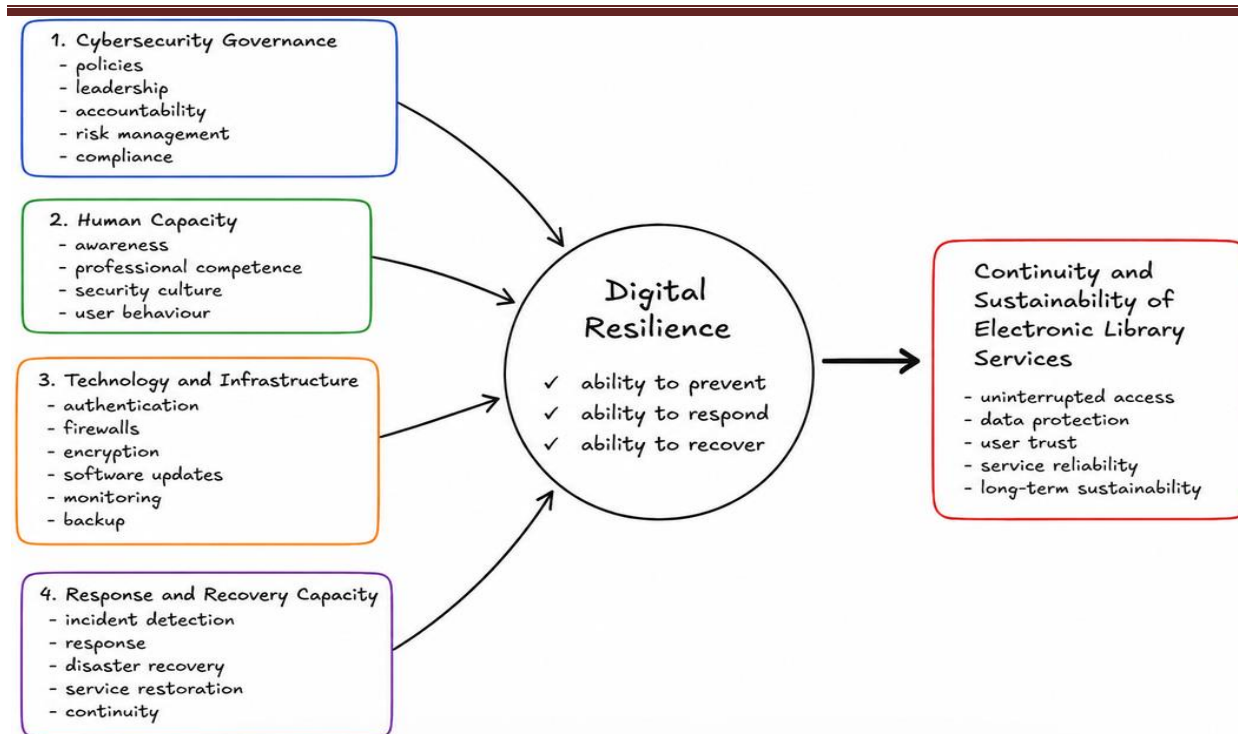


Fig 1: Conceptual Framework

The above conceptual framework illustrates how above four interconnected dimensions interact to promote Digital Resilience which in turn supports Continuity and Sustainability of Electronic Library Services. The framework therefore adopts the following logic:

Cybersecurity Governance + Human Capacity + Technology/Infrastructure + Response & Recovery → Digital Resilience → Continuity of Electronic Library Services.

Essentially, the conceptual contribution of this model portrays service continuity as the goal while cybersecurity is a means. Therefore, this study aligns with modern resilience approach by focusing on organizational ability to continue basic functions of quick recovery and enhance preparedness after disruptions (Mahmood et al., 2024; Lee, 2025).

3. METHODOLOGY

Research Design and Study Context

The study adopted a mixed-methods research design to examine how cybersecurity governance, human capacity, technology and infrastructure, response and recovery capacity influence digital resilience and the continuity of electronic library services. The mixed-methods approach was appropriate because cybersecurity in university libraries involves both measurable organizational practices and contextual human and institutional experiences. It also allows quantitative evidence to be complemented by qualitative observations and professional perspectives, thereby providing a comprehensive basis for framework development. Methodological reviews have shown that mixed methods can strengthen the breadth, depth and corroboration of evidence in library and

information science research when the quantitative and qualitative components are appropriately integrated (Liu, 2020).

This study was conducted in South-South Nigeria, where university libraries depend on electronic journals, databases, institutional repositories, e-books, online discovery systems and network information services. The study covered 10 university libraries, comprising six Federal, two State and two Private universities. This institutional spread provided representation across various ownership structures and provided a useful basis for examining whether cybersecurity and resilience challenges extended beyond individual institutional settings. The choice of context was also supported by relevant Nigerian and African findings by identifying malware, phishing, ransomware, identity theft, inadequate infrastructure and limited cybersecurity capacity as important issues for university libraries (Igbinovia & Ishola, 2023 and Oladokun et al., 2024).

Population, Sample and Sampling Techniques

The target population comprise library staff involved in the management, provision, maintenance and use of electronic library resources and related digital services in selected university libraries. The study used a sample of 200 respondents from 10 participating university libraries. The institutional sample comprised six Federal, two State and two Private universities, thereby capturing three major university ownership categories in the study area. Respondents were selected because their professional responsibilities provided direct exposure to electronic-resource management, information security practices, user access, ICT systems and service continuity.

A structured questionnaire was administered to 200 selected respondents, while selected library staff and relevant ICT-related observations provided qualitative evidence for interpreting survey results. Out of the 200 questionnaires administered, 161 were validly completed and returned, representing an 80.5% response rate. The response level was considered adequate for the analysis and was higher than the level at which non-response could compromise interpretation. The use of library staff as the principal respondents was consistent with Nigerian findings showing that library staff constitute an important source of information on institutional cybersecurity practices and preparedness (Igbinovia & Ishola, 2023).

Instrument, Validity and Reliability

Data were collected using a structured instrument titled Questionnaire on Cybersecurity Governance, Digital Resilience and Continuity of Electronic Library Services (QCGDRCELS). The questionnaire items were developed from study objectives, socio-technical perspective and relevant cybersecurity literature. The instrument measured four principal dimensions: cybersecurity governance, human capacity, technology and infrastructure, response and recovery capacity, together with indicators of digital resilience and continuity of electronic library services. Content and face validity were established through expert assessment. The instrument was reviewed for clarity, relevance, coverage of study constructs and alignment between questionnaire items and conceptual framework. This was crucial because cybersecurity research in African university libraries highlighted interconnected nature of technological, human, policy and institutional vulnerabilities rather than treating cybersecurity as a separate technical issue (Oladokun et al., 2024). Reliability was assessed using Cronbach's alpha, with coefficients of 0.70 or above regarded as acceptable for the study constructs. This procedure provided evidence that the items measuring each construct demonstrated adequate internal consistency before the main

analysis was undertaken.

Data Collection and Analysis

Data was collected through direct administration of questionnaire supplemented by interviews and structured observations of relevant electronic-resource security practices. The qualitative component focused on institutional policies, staff awareness, authentication arrangements, backup practices, incident response and mechanisms for restoring electronic library services following disruptions. The 161 valid questionnaire responses were analyzed using frequency counts, percentages, Mean ($\bar{x}$) and Standard Deviation (SD). These descriptive techniques were used to establish the prevalence of cybersecurity practices, perceived institutional capacity and major factors associated with digital resilience and service continuity. Qualitative evidence was analyzed thematically to explain, corroborate and contextualize quantitative findings. This integration was important because previous LIS methodological research has cautioned that simply combining quantitative and qualitative data without meaningful integration weakens contribution of mixed-methods studies (Liu, 2020).

Framework Development and Validation

The Institutional Cyber-Resilience Framework was developed by synthesizing empirical findings with socio-technical systems perspective. The framework portrayed cybersecurity governance, human capacity, technology and infrastructure, response and recovery capacity as interdependent organizational capabilities rather than isolated security measures. The symbiotic interaction was conceptualized as producing digital resilience which supports continuity and sustainability of electronic library services.

Figure 1 presents the proposed conceptual relationship among study variables. The framework recognized effective cybersecurity dependence not only on technical controls but on leadership, institutional accountability, staff competence, security culture, funding, policies and the capacity to detect, respond and recover from cyber incidents. This position is consistent with African evidence requesting for stronger cybersecurity education, cyberethics policies, technological investment and institutional resilience in university libraries (Oladokun et al., 2024 and Akor et al., 2024). The framework was also subjected to expert validation to assess relevance, clarity, logical consistency and practical applicability of the four dimensions and relationships. Feedback from the validation process was used to refine the framework and ensure that it reflected operational realities of university libraries in South-South Nigeria. The resulting framework therefore moved beyond identifying cyber threats to provide an institutionally grounded model for prevention, preparedness, response, recovery and continuity of electronic library services.

4. RESULTS

Descriptive Findings

Data from 161 valid respondents was analyzed to establish prevailing conditions of cybersecurity governance, digital resilience and continuity of electronic library services. Responses were measured on a five-point Likert scale, where higher scores indicated stronger institutional practices or greater agreement with the statements. The descriptive results indicated that cybersecurity practices existed in sampled university libraries, but their implementation was not uniformly

strong. In particular, governance mechanisms, staff capacity and incident-response arrangements appeared less developed than basic technological controls.

Table 1: Descriptive Statistics of Study Variables (N = 161)

Study Variable	Mean ($\bar{x}$)	SD	Remarks
Cybersecurity Governance	3.18	0.71	Moderate
Human Capacity	3.05	0.76	Moderate
Technology and Infrastructure	3.27	0.69	Moderate
Response and Recovery Capacity	2.91	0.81	Moderate
Digital Resilience	3.12	0.73	Moderate
Continuity of Electronic Library Services	3.24	0.70	Moderate
Grand Mean	3.13	0.73	Moderate

Criterion mean = 3.00.

The results revealed that technology and infrastructure recorded the highest ($\bar{x} = 3.27$), followed by continuity of electronic library services ($\bar{x} = 3.24$, $SD = 0.70$) and cybersecurity governance ($\bar{x} = 3.18$, $SD = 0.71$). However, response on recovery capacity recorded the lowest ($\bar{x} = 2.91$, $SD = 0.81$) suggesting relative weakness in the ability of libraries to detect, contain, recover from and learn from cybersecurity incidents. This distinction is important because the availability of firewalls, authentication systems and software protection does not necessarily demonstrate institutional resilience. Similarly, Igbinovia & Ishola, (2023) and Oladokun et al., (2024) findings revealed that university libraries experience cybersecurity challenges associated with inadequate infrastructure, technical skills, funding and institutional preparedness.

Table 2: Cybersecurity Governance Indicators (N = 161)

Cybersecurity Governance Indicator	Mean	SD	Rank
University has formal cybersecurity policies	3.29	0.82	1
Library management provides security oversight	3.24	0.78	2
Access to electronic resources is controlled	3.21	0.76	3
Cybersecurity responsibilities are clearly defined	3.13	0.81	4
Regular cybersecurity risk assessments are conducted	3.05	0.84	5
Formal incident-reporting procedures exist	2.98	0.86	6
Grand Mean	3.15	0.81	

Note: criterion mean = 3.00.

Table 2 revealed that the strongest governance feature was the existence of formal cybersecurity policies ($\bar{x} = 3.29$, $SD = 0.82$), while formal incident-reporting procedures recorded the lowest ($\bar{x} = 2.98$, $SD = 0.86$). This suggests potential governance–implementation gap. This implies that institutions may have policies on paper without equivalent capacity for systematic risk assessment, incident reporting and organizational learning. This gap is significant because effective cybersecurity governance requires leadership, accountability, risk management and continuous monitoring rather than separate policy formulation. This finding supports Malatji et al., (2019) that socio-technical protection is unlikely to be sustainable where organizational structures and human responsibilities are weak.

Table 3: Digital Resilience and Continuity of Electronic Library Services (n = 161)

Indicator	Mean	SD	Remarks
Library can maintain essential electronic services during cyber incidents	3.31	0.75	Moderate
Electronic resources can be restored after disruption	3.27	0.79	Moderate
Regular data backup is maintained	3.34	0.73	Moderate
Alternative access arrangements are available	3.02	0.82	Moderate
Staff can respond quickly to service disruption	2.96	0.85	Moderate
Recovery procedures are periodically tested	2.88	0.87	Moderate
Electronic services are continuously monitored	3.18	0.76	Moderate
Grand Mean	3.14	0.79	Moderate

Note: criterion Mean = 3.00.

Table 3 revealed regular data backup ($\bar{x} = 3.34$, $SD=0.73$) and the ability to maintain essential electronic services during cyber incidents ($\bar{x} = 3.31$, $SD=0.75$) were relatively stronger. However, recovery-procedure testing ($\bar{x} = 2.88$, $SD=0.87$) and staff response capability ($\bar{x} = 2.96$, $SD=0.85$) were comparatively weak. The pattern indicates that sampled libraries were more oriented towards protection and basic preparedness than tested recovery and adaptive resilience. This is a critical finding because service continuity depends not simply on preventing attacks but on capacity to restore access rapidly when preventive controls fail. The findings of Oladokun et al., (2024) identified cybersecurity preparedness and institutional capacity as important issues for university libraries. These findings suggest that digital resilience should be understood as an institutional capability rather than a collection of isolated technical controls. These moderate scores revealed that South-South Nigerian university libraries have begun implementing cybersecurity measures but lack comprehensive resilient. This finding provides the empirical basis for developing Institutional Cyber-Resilience Framework, which integrates governance, human capacity, technology and infrastructure, response and recovery into an integrated system for sustaining electronic library services.

5. DISCUSSION

The findings revealed that cybersecurity in university libraries in South-South Nigeria is a multidimensional institutional challenge shaped by symbiotic interactions between technological, human and organizational factors. Malware was the most prevalent cyber threat (64.0%), followed by password cracking/password theft (58.4%), unauthorized data copying and data breaches (57.1% respectively), ransomware (54.0%) and social engineering (53.4%). The overall availability of identified cyber threats (51.1%) was marginally higher than non-availability (48.9%), indicating a fragile rather than uniformly secure or insecure cybersecurity environment. This findings confirmed Ajie (2019) that identified malware, hacking and unauthorized access are critical issues in university libraries. Likewise, Njoku et al. (2023) found that vulnerabilities involve identity management, infrastructure and data protection in Nigerian institutional repositories. The prominence of malware and credential-related threats further revealed that electronic-resource security cannot be addressed through separate technology because password theft, phishing and social engineering exploit weaknesses in human behaviour and security practices.

Similarly, Igbinovia & Ishola (2023) found that limitations in cybersecurity knowledge among Nigerian university library staff. However, the present findings also revealed that knowledge deficits of cybersecurity awareness must be translated into organizational capability through effective governance, infrastructure, monitoring and response mechanisms. The overall awareness ($\bar{x}$ = 2.52) is marginally above ($\bar{x}$ = 2.50) criterion mean should not be interpreted as strong preparedness. Respondents showed greater awareness of visible threats such as unauthorized data copying and data breaches ($\bar{x}$ = 2.73) while there is lower awareness of technically complex threats such as supply-chain attacks ($\bar{x}$ = 2.21), code injection ($\bar{x}$ = 2.24), pharming ($\bar{x}$ = 2.27), remote-work security risks ($\bar{x}$ = 2.32) and spoofing ($\bar{x}$ = 2.34). This reveals that basic recognition of cybersecurity threats does not necessarily translate into competence required to identify sophisticated and emerging attack vectors.

The findings concerning institutional challenges provide an important explanation for awareness-preparedness gap. The grand mean ($\bar{x}$ = 3.04) reveals that cybersecurity is constrained by institutional and resource-related limitations, particularly high security-software costs ($\bar{x}$ = 3.24), inadequate funding ($\bar{x}$ = 3.22), inadequate cybersecurity awareness ($\bar{x}$ = 3.19), inadequate ICT infrastructure ($\bar{x}$ = 3.14) and insufficient technical knowledge and skills (approximately $\bar{x}$ = 3.08–3.09). These result support Igbinovia & Ishola (2023) findings that cybersecurity limitations in Nigerian university libraries have deficiencies in knowledge and institutional capacity. This is in tandem with Njoku et al. (2023) findings that infrastructure, identity-management and data-protection weaknesses affect cybersecurity in libraries. These findings also agreed with Aminikpo & Okwu (2025) that inadequate infrastructure, limited technical skills and insufficient training affect university-library cybersecurity in Rivers State, Nigeria. Nevertheless, respondents strongly recognized appropriate mitigation measures with grand mean ($\bar{x}$ = 3.08) to include strong passwords ($\bar{x}$ = 3.27), regular software updates ($\bar{x}$ = 3.26), staff training ($\bar{x}$ = 3.23), link verification ($\bar{x}$ = 3.21), user training ($\bar{x}$ = 3.19), secure browsing ($\bar{x}$ = 3.18), multifactor authentication ($\bar{x}$ = 3.15), backup and encryption ($\bar{x}$ = 3.14 respectively) and firewalls ($\bar{x}$ = 3.12) were strongly endorsed.

These findings also support Mosteiro-Sanchez et al. (2020), Mukdasanit & Kantabutra (2021) and NIST (2024) that Defence-in-Depth multiple complementary layers of protection rather than reliance on a single security mechanism for cybersecurity are continuous process involving governance, identification, protection, detection, response and recovery. However, the comparatively weaker ratings for awareness programmes ($\bar{x}$ = 2.70) and adequate funding ($\bar{x}$ = 2.81) revealed that awareness-capacity-implementation paradox: as respondents understand what should be done but institutional challenges limit what can be implemented. Findings also aligned with Ezeabasili & Nwosu (2018) that availability of electronic security technologies does not necessarily guarantee utilization. Consequently, the acquisition of firewalls, antivirus software, encryption or authentication technologies cannot independently guarantee secure electronic-resource environments rather their effectiveness depends on maintenance, competent personnel, funding, user compliance and organizational enforcement.

Furthermore, the comparison of existing findings revealed high prevalence of malware, password-related attacks, data breaches and unauthorized copying. These findings agreed with Ajie (2019), Okike & Adetoro (2019) and Njoku et al. (2023) that hacking, malware, unauthorized access and intellectual-property risks are prevalent in Nigerian academic information environments. However, the present study found that vulnerability is substantial but not universal (51.1%) of

available threats. This implies that university libraries in South-South Nigeria should not be treated as homogeneous cybersecurity environments because of differences in ownership, funding, ICT maturity, management support, technical expertise and library practices at various levels of exposure. Likewise, Aminikpo & Okwu (2025) findings revealed that network, system and application security are associated with protection of online library environments in Rivers State, Nigeria while infrastructure and skills limitations remain significant. Additionally, the findings on awareness also supports Igbinovia & Ishola (2023) findings that awareness constitutes adequate preparedness ($\bar{x} = 2.52$) of supply-chain attacks, code injection, pharming and spoofing need continuous, role-specific and threat-specific cybersecurity education. Therefore, the findings of Mosteiro-Sanchez et al.(2020), Mukdasanit & Kantabutra (2021) and NIST (2024) confirmed strong support for MFA, software updates, training, encryption, backups and firewalls are compatible with Defence-in-Depth approach cybersecurity lifecycle. Besides, results revealed that recognition of layered security controls is stronger than institutional capacity required for sustenance. Significantly, this study supports findings on appropriate layered cybersecurity. Contrarily, the effectiveness in local context would depend on whether universities have resources, personnel, policies and processes required to finance, implement, monitor and update these factors. Furthermore, the basic theoretical contribution of this study is embedded in Socio-Technical Systems Theory of Trist & Bamforth (1951) and Emery & Trist (1960) that organizational effectiveness depends on the interaction and joint optimization of social and technical subsystems rather than technological solutions operating in isolation. Thus, this submission agreed with findings of the present study in university libraries in South-South Nigeria that technical subsystem includes databases, networks, authentication systems, firewalls, encryption and backup systems, while social and organizational subsystem encompasses librarians, users, ICT personnel, management, policies, funding, training and institutional practices. Similarly, the findings of Malatji et al. (2019) that cybersecurity is a socio-technical phenomenon that must be integrated with human and organizational factors. Therefore, the integration of cybersecurity technologies, marginal awareness, insufficient expertise, inadequate infrastructure and funding challenges revealed that electronic-resource security generates intimate interactions between these dimensions. Notably, cybersecurity is required for the protection of digital resilience to prevent attacks and detect incidents, respond effectively, recover affected systems, protect data and maintain continuity of scholarly access. This supports NIST (2024) findings that provide a conceptual basis for understanding how cybersecurity governance, human capacity, technology and infrastructure, response and recovery capacity can collectively strengthen digital resilience and continuity of electronic library services in university libraries in South-South Nigeria.

Essentially, the practical contributions of this study affirmed that university management should move from fragmented cybersecurity expenditure towards integrated cybersecurity governance due to inadequate funding ($\bar{x} = 3.22$). Hence, cybersecurity should be incorporated into routine institutional and library budgeting rather than as an emergency ICT expense. Investment should prioritize authentication systems, electronic databases, institutional repositories, network infrastructure, backup systems and staff development. Library management should also institutionalize formal cybersecurity policies specifying responsibilities for management, librarians, ICT personnel and users. These provisions should also cover authentication, privileged access, MFA, remote access, data protection, software updates, backups, incident reporting and third-party electronic-resource services. Moreover, cybersecurity competence should become part

of continuing professional development because librarians function as custodians of digital resources, user identities, access credentials and scholarly information. Consequently, interventions should be context-sensitive rather than replicating models from highly resourced environments for university libraries in South-South, Nigeria. Results also revealed that funding limitations, infrastructure deficiencies, uneven technical capacity and varying levels of cybersecurity awareness can restrict implementation. Therefore, the most appropriate intervention is not necessarily technologically sophisticated solution but institutionalized, maintained and continuously improved available resources.

This study identifies awareness–capacity–implementation paradox that library staff acknowledge cyber threats and support safeguards, but institutional limitations hinder implementation of effective cybersecurity measures. These findings support a shift from isolated awareness programmes and technology acquisition towards an integrated digital-resilience framework based on joint optimization of cybersecurity governance, human capacity, technology and infrastructure, response and recovery capability, organizational learning and sustainable funding. This present study is theoretically grounded in Socio-Technical Systems Theory (Trist & Bamforth, 1951; Emery & Trist, 1960 and Malatji et al., 2019) and practically align with Mosteiro-Sanchez et al. (2020) and NIST (2024) layered protection and continuous risk management. These provided fertile landscape for improving continuity, reliability and sustainability of electronic library services in South-South, Nigeria.

Table 4: Pearson Correlation Matrix among Study Variables (N = 161)

Variables	1	2	3	4	5	6
1. Cybersecurity Governance	1.00					
2. Human Capacity	.58**	1.00				
3. Technology & Infrastructure	.64**	.51**	1.00			
4. Response & Recovery Capacity	.61**	.55**	.68**	1.00		
5. Digital Resilience	.72**	.66**	.74**	.76**	1.00	
6. Service Continuity	.65**	.59**	.69**	.73**	.81**	1.00

Note. $p < .01$, two-tailed.

Table 4 shows positive and statistically significant relationships among all six variables. Digital resilience was strongly associated with response and recovery capacity ($r = .76$), technology and infrastructure ($r = .74$) and cybersecurity governance ($r = .72$). Its strongest relationship was with continuity of electronic library services ($r = .81$) revealing that libraries with stronger capacities to anticipate, withstand, respond and recover from cyber disruptions were more likely to sustain electronic services. The findings agreed with studies from Nigerian university libraries that service sustainability depends on adequate funding, infrastructure, technical capacity and institutional strategies (Eneh et al., 2023).

Table 5: Multiple Regression Predicting Digital Resilience (N = 161)

Predictor	B	SE	β	t	p
Constant	0.61	0.24	—	2.54	.012
Cybersecurity Governance	0.21	0.07	.23	3.12	.002
Human Capacity	0.18	0.07	.19	2.67	.008
Technology & Infrastructure	0.27	0.08	.29	3.44	<.001

Response & Recovery Capacity	0.31	0.08	.34	3.91	<.001
------------------------------	------	------	-----	------	-------

$R^2 = .68$; *Adjusted R*² = .67; $F_{(4, 156)} = 82.71$, $p < .001$

The regression model result in Table 5 was statistically significant and explained 68% of variance in digital resilience. Response and recovery capacity made the strongest independent contribution ($\beta = .34$), followed by technology and infrastructure ($\beta = .29$), cybersecurity governance ($\beta = .23$) and human capacity ($\beta = .19$). Results revealed that cyber-resilience is not simply a function of acquiring security technologies; it also requires institutional preparedness, skilled personnel and capacity to respond effectively when disruption occurs. This finding agrees with socio-technical cybersecurity perspective that there exist an intimate interactions between social, technical and organizational elements in security management in libraries (Malatji et al., 2019).

Table 6: Regression Effect of Digital Resilience on Continuity of Electronic Library Services (N = 161)

Predictor	B	SE	β	t	p
Constant	0.74	0.21	—	3.52	<.001
Digital Resilience	0.79	0.06	.81	12.94	<.001

$R^2 = .66$; *Adjusted R*² = .66; $F_{(1, 159)} = 167.44$, $p < .001$

From Table 6 Digital resilience significantly predicted continuity of electronic library services ($\beta = .81$, $p < .001$), accounting for 66% of the observed variance. This reveals that resiliencies a vital pathway through which governance, human capacity, technological capability and recovery mechanisms translate into sustained electronic library services. This finding is significant in the Nigerian context because current findings continues to identify infrastructure, funding, user awareness and institutional capacity as important challenges that affect digital library accessibility and sustainability (Idhalama et al., 2025; Eneh et al., 2023).

Development and Validation of Institutional Cyber-Resilience Framework

The empirical findings provided the basis for developing Institutional Cyber-Resilience Framework (ICRF). The framework integrated four mutually reinforcing institutional capabilities—cybersecurity governance, human capacity, technology and infrastructure and response and recovery capacity as principal drivers of digital resilience. Digital resilience was positioned as immediate mechanism through which these capabilities support continuity and sustainability of electronic library services. This model adapts the socio-technical perspective to create a library-specific resilience framework (Malatji et al., 2019).

Table 7: Expert Validation of Institutional Cyber-Resilience Framework

Framework Components	Mean	SD	Decision
Cybersecurity Governance	4.42	0.51	Accepted
Human Capacity	4.36	0.55	Accepted
Technology and Infrastructure	4.48	0.50	Accepted
Response and Recovery Capacity	4.51	0.50	Accepted
Digital Resilience	4.55	0.50	Accepted
Continuity of Electronic Library Services	4.58	0.50	Accepted
Overall Framework	4.48	0.51	Validated

Note. Scale: 1 = Very Inappropriate; 5 = Very Appropriate. Criterion mean = 3.00.

The validation results revealed strong expert agreement on the relevance and applicability of proposed framework. The overall mean ($\bar{x} = 4.48$, $SD = 0.51$) was greater than the criterion mean of ($\bar{x} = 3.00$). Continuity of electronic library services recorded the highest rating ($\bar{x} = 4.58$, $SD = 0.50$), followed by digital resilience ($\bar{x} = 4.55$, $SD = 0.50$) revealing that experts accepted sustained service delivery as the ultimate institutional outcome of cybersecurity investment. These findings agreed with current studies advocating for strategic intervention in infrastructure, funding, policy and capacity development to improve availability and accessibility of digital library services in Nigeria. The framework logic reveals that the addition of cybersecurity Governance, human capacity, technology and infrastructure, response and recovery capacity will lead to digital resilience and positively impact continuity and sustainability of electronic library services. Therefore, the primary contribution of the framework is a shift from a threat-prevention model to an institutional resilience model. Rather than treating cybersecurity as the responsibility of ICT personnel, the framework assigns shared responsibility to library leadership, librarians, ICT professionals, users and university management. This is relevant in Nigerian universities, where sustainability of electronic resources is affected by interconnected organizational, infrastructural and human challenges (Eneh et al., 2023 and Idhalama et al., 2025).

6. POLICY IMPLICATIONS

The findings of this study implies that cybersecurity should be repositioned from a narrow ICT responsibility to a core institutional governance and service-continuity priority in the management of university libraries. The relatively high prevalence of malware, password-related attacks, data breaches and social engineering, combined with marginal cybersecurity awareness, funding, infrastructure and skills challenges revealed that reactive technology-only approaches are inadequate. Therefore, university management should establish formal cybersecurity governance structures that clearly assign responsibilities to management, library administrators, ICT personnel and users, supported by dedicated and recurrent funding. Libraries should develop and enforce policies covering authentication, multifactor authentication, privileged access, remote access, data protection, software updates, backups, incident reporting and third-party electronic-resource platforms. Cybersecurity training should be continuous, role-specific and threat-sensitive. The policy priority should integrate people, processes and technology so that security controls are not merely acquired but consistently implemented, monitored, evaluated and improved. This aligns with the socio-technical interpretation of cybersecurity advanced by Trist & Bamforth (1951), Emery & Trist (1960) and Malatji et al. (2019) to support continuous governance, protection, detection, response and recovery orientation of NIST (2024).

In addition, TETFund and other relevant regulatory agencies found that there is need for a stronger funding and regulatory framework that treats cybersecurity and digital continuity as essential components to enhance contemporary university infrastructure. Therefore, the major challenges of this study include inadequate funding, high security-software costs, insufficient ICT infrastructure and limited technical skills that cannot be effectively addressed by university libraries. Thus, TETFund should fund cybersecurity infrastructure, staff development and security assessments. The funding criteria should move beyond procurement of equipment to include evidence of implementation, maintenance, staff competence, incident-response capability and sustainability. Regulatory agencies should set minimum cybersecurity standards to include institutional capacity and financial requirements for university libraries. This approach would enhance institutional

cybersecurity maturity and digital resilience. In essence, cybersecurity policy should ensure digital continuity and preventive measures. Findings of this study also revealed that universities should address gaps in awareness-implementation by prioritizing cybersecurity to focus on resources, risk assessment, layered security, staff competence, incident response and access to information. This should also include reliable backups, recovery tests, monitoring, updates, authentication, and documented incident plans. Hence, digital continuity should be incorporated into institutional risk-management and strategic-planning frameworks to prevent cybersecurity disruptions and potential threats to teaching, research, accreditation and institutional reputation. This implies that policy effectiveness will depend on adopting sophisticated technologies for selecting sustainable controls to finance, operate and continuously improve university libraries in South-South, Nigeria. The policy should also focus on resilient library systems that ensure continuity of electronic resources through prevention, detection, response and recovery from cyber incidents, prioritizing institutional resilience over technology protection.

7. CONCLUSION AND RECOMMENDATIONS

This study concludes that cybersecurity in university libraries in South-South Nigeria is characterized by exposure to cyber threats, marginal cybersecurity awareness, inadequate infrastructure, funding and limited technical capacity. Although, library personnel strongly recognized appropriate protective measures, the gap between awareness and implementation hinder effective protection and continuity of electronic-resource services. Therefore, cybersecurity is a socio-technical and institutional resilience issue that requires integration of governance, human capacity, technology, response capability and sustainable funding. University management should establish dedicated cybersecurity governance structures, advocate for sustainable funding, strengthen authentication, backup systems and continuous cybersecurity training for library and ICT personnel. Libraries should implement formal cybersecurity and incident-response policies, conduct regular risk assessments, update security systems and test recovery procedures. TETFund and regulatory agencies should also provide dedicated support for cybersecurity infrastructure, staff capacity development and digital-continuity initiatives by establishing cybersecurity standards for university libraries. These measures should prioritize sustainable implementation rather than technology acquisition.

8. LIMITATIONS AND FUTURE RESEARCH

This study is limited to university libraries in South-South Nigeria and relied primarily on respondents' reported perceptions and practices, which may not fully capture actual cybersecurity incidents or technical vulnerabilities. Future studies should employ longitudinal and mixed-method designs, incorporate technical security assessments and compare cybersecurity maturity across Nigerian geopolitical zones and university ownership types. Further research should also examine how cybersecurity governance and digital resilience influence continuity and sustainability of electronic library services.

Acknowledgement

Authors gratefully acknowledge the Tertiary Education Trust Fund (TETFund), FCT Abuja, for the financial sponsorship and support provided for this research project. The financial support provided through the research funding made it possible to undertake the study including necessary

research activities, data collection, analysis and dissemination of findings. The authors sincerely appreciate this support and recognize TETFund's important contribution to advancing evidence-based research and promoting sustainable development in Nigerian's higher education sector.

REFERENCES

- Akor, S. O., Nongo, C. J., Udofot, C. O. & 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*, 2. <https://doi.org/10.25159/3005-4222/16671>
- Cervone, H. F. (2006). Disaster recovery and continuity planning for digital library systems. *OCLC Systems & Services: International Digital Library Perspectives*, 22(3), 173-178. <https://doi.org/10.1108/10650750610686234>
- Emery, F. E. & Trist, E. L. (1960). Socio-technical systems. In C. W. Churchman & M. Verhulst (Eds.), *Management sciences, models and techniques* (2), 83-97. Pergamon Press.
- Eneh, A. C., Ukachi, N. B., Ibikunle, G. O. & Sambe, M. T. (2023). Strategies for sustaining digital libraries and electronic information resources: A survey of Nigerian universities. *Niger Delta Journal of Library and Information Science*, 4(1), 11-22.
- Idhalama, O. U., Oredo, J. O. & Makori, E. O. (2025). Evaluating the availability and accessibility of digital resources and services in public university libraries in Nigeria. *Alexandria: The Journal of National and International Library and Information Issues*, 35(1-2), 89-103. <https://doi.org/10.1177/09557490251335954>
- Igbinoia, 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>
- Lee, P.C. (2025). Navigating the path to sustainability: Digital resilience in libraries. *Journal of Librarianship and Information Science*. <https://doi.org/10.1177/03400352251331465>
- Liu, Y. (2020). Mixed methods research in library and information science: A methodological review. *Library & Information Science Research*.
- Mahmood, M. et al. (2024). Digital resilience framework for managing crisis: A qualitative study in the higher education and research sector. *Journal of Contingencies and Crisis Management*.
- Malatji, M., von Solms, S. & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, 27(2), 233-272. <https://doi.org/10.1108/ICS-03-2018-0031>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.29>
- Njoku, I. S., Njoku, B. C., Chukwu, S. A. J. & Ravichandran, R. (2023). Fostering cybersecurity in institutional repositories: A case of Nigerian universities. *African Journal of Library, Archives and Information Science*, 33(1), 1-21.
- Oladokun, B. D., Oloniruha, E. A., Mazah, D. & Okechukwu, O. C. (2024). Cybersecurity risks: A sine qua non for university libraries in Africa. *Southern African Journal of Security*, 2, 1-14. <https://doi.org/10.25159/3005-4222/15320>
- Pascoe, C., Quinn, S. & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.29>