International Journal of Information Resource Management (IJIRM)

Volume 2, Number 3 (2025)

E- ISSN: 1118-7786

# CYBER SECURITY MEASURES FOR OPTIMIZED SERVICE DELIVERY IN FEDERAL UNIVERSITY LIBRARIES IN NORTH-EAST, NIGERIA

**By**

**TAMA T.A TIMOKO CLN**
**and**

**LAWRENCE OGAH CLN**

## Abstract

This study examined the Cyber Security measures employed in federal university libraries in North East Nigeria and their impact on service delivery. A descriptive survey design was utilized, with a sample of 60 library and ICT staff selected from four federal universities in the region through purposive sampling. Data were gathered using a structured questionnaire and analyzed using descriptive and inferential statistical methods. The findings revealed that while a majority of libraries had basic Cyber Security measures in place, such as firewalls and antivirus software (85% and 78% respectively), advanced measures like data encryption and intrusion detection systems were underutilized (18% and 22%). Additionally, 60% of respondents reported experiencing at least one Cyber Security breach in the last two years. A positive correlation ($r = 0.68$, $p < 0.05$) was found between the extent of Cyber Security implementation and the quality of library service delivery, indicating that better Cyber Security practices lead to improved service efficiency. Major challenges identified included inadequate funding (72%), insufficient training (43%), and outdated ICT infrastructure (68%). The study highlighted the importance of robust Cyber Security frameworks in enhancing library operations and protecting digital resources. Based on the findings, the study recommended the development of formal Cyber Security policies, investment in advanced security technologies, regular staff training, and increased institutional support to optimize service delivery and safeguard academic resources.

**Keywords**: Cyber Security Measures, Service Delivery, Federal University Libraries, North East Nigeria, Library Services.

## Introduction

In the contemporary digital landscape, university libraries play a pivotal role in the academic and research development of higher institutions. These libraries have increasingly embraced digital technologies and automated systems to facilitate access to vast information

resources, streamline operations, and improve user experience. Particularly in federal university libraries, where service delivery is expected to meet national educational standards, the integration of information and communication technologies (ICTs) has become indispensable. However, this digital shift has brought about heightened concerns over Cyber Security, especially in developing regions like North East Nigeria, where infrastructural limitations and security vulnerabilities are prevalent (Okite-Amughoro et al., 2020).

Cyber Security in academic libraries refers to the policies, processes, and technologies used to protect digital assets, such as library databases, online catalogs, and user information, from unauthorized access, cyberattacks, and data breaches. As federal university libraries continue to transition from traditional to electronic library systems, they become increasingly exposed to various cyber threats, including ransomware, phishing, denial of service (DoS) attacks, and insider threats (Eze & Uzoigwe, 2022). These threats not only compromise the integrity and confidentiality of data but also disrupt library services, erode user trust, and hinder academic productivity.

In North East Nigeria, universities face unique challenges due to the region's socio-economic instability, infrastructural deficiencies, and limited investment in digital infrastructure. These factors collectively contribute to weak Cyber Security frameworks and make university libraries particularly vulnerable. Moreover, studies have shown that many academic libraries in the region operate without comprehensive Cyber Security policies, and library staff often lack adequate training in information security (Babalola & Adebayo, 2021). This knowledge gap, coupled with outdated security systems and limited financial resources, undermines the ability of libraries to deliver optimized and uninterrupted services to users.

As higher education institutions increasingly depend on digital systems for scholarly communication, e-resources management, and academic collaboration, ensuring the security of these systems becomes not only a technical priority but a strategic imperative. Therefore, there is an urgent need to assess the existing Cyber Security measures in federal university libraries in North East Nigeria, identify areas of vulnerability, and propose strategic improvements that align

with international best practices. This study seeks to bridge this gap by examining current Cyber Security practices, evaluating their effectiveness in promoting efficient service delivery, and recommending context-specific measures for enhancing the resilience of academic libraries against cyber threats.

**Problem Statement**

Despite the increasing adoption of digital technologies in university libraries across Nigeria, Cyber Security remains a significant and often under-addressed challenge, particularly in the federal university libraries situated in the North East region. These libraries serve as critical academic hubs, supporting teaching, learning, and research by offering access to digital resources, online databases, and automated library systems. However, their growing reliance on technology has made them more susceptible to various forms of cyberattacks such as malware infections, phishing scams, data breaches, and system intrusions (Eze & Uzoigwe, 2022).

Unfortunately, many of these libraries lack robust Cyber Security infrastructures, comprehensive risk management strategies, and well-trained personnel to handle digital security challenges effectively (Babalola & Adebayo, 2021). Furthermore, the prevailing socio-political instability in the North East, coupled with limited funding and inadequate ICT policies, exacerbates the situation by hindering the implementation of proactive Cyber Security measures. As a result, these libraries are frequently exposed to threats that not only compromise the integrity and confidentiality of user data but also disrupt information service delivery, reduce operational efficiency, and potentially damage the credibility of academic institutions. Despite the critical nature of these issues, there remains a dearth of empirical research focused on assessing the Cyber Security preparedness and practices of federal university libraries in this region.

This study, therefore, seeks to fill this gap by investigating the current state of Cyber Security measures in federal university libraries in North East Nigeria, evaluating their effectiveness, and determining their impact on service delivery. The findings are expected to

inform policy decisions, improve digital security frameworks, and promote optimized library services in the region.

**Research Questions**

1. What types of cyber security measures are currently available and implemented in federal university libraries in North East Nigeria?
2. To what extent are library staff and users aware of cyber security threats and preventive practices?
3. How effective are the existing Cyber Security measures in ensuring the integrity, confidentiality, and availability of digital library services?
4. What are the major challenges facing the implementation of effective Cyber Security strategies in these libraries?
5. How do Cyber Security practices impact the overall quality and efficiency of service delivery in federal university libraries in North East Nigeria?
6. What recommendations can be made to enhance Cyber Security and optimize service delivery in academic libraries within the region?

**Literature Review**

Cyber Security is increasingly recognized as a strategic necessity in academic libraries, especially with the rapid digitization of information systems. In the context of federal university libraries in Nigeria, this shift toward digital operations has introduced both opportunities and vulnerabilities. Effective Cyber Security encompasses the use of tools, policies, and practices designed to protect library systems and user data from unauthorized access, data corruption, and service disruption (Eze & Uzoigwe, 2022; Okike, 2021).

Nigerian academic libraries face a unique set of challenges due to insufficient infrastructure, poor policy implementation, and underfunding. According to Ajegbomogun and Salaam (2019), many library professionals lack adequate Cyber Security knowledge, increasing their exposure to threats such as phishing, malware, and data breaches. Tella and Oguntayo (2020)

further observed that institutional attitude and staff commitment significantly affect the success of Cyber Security initiatives.

Outdated ICT infrastructure is another core issue. In a study of selected Nigerian university libraries, Okite-Amughoro et al. (2020) found that most digital systems were inadequately maintained, making them vulnerable to intrusion. This finding is echoed by Azeez and Oyelude (2022), who reported that poor network reliability and obsolete hardware often hinder proactive security practices.

Cyber Security awareness is vital in building a resilient digital environment. Ogunmodede and Akintola (2020) revealed that the absence of structured training for library staff contributes to low detection and poor incident response rates. Abubakar and Muhammad (2021) confirmed that in North-East Nigeria, many library personnel were unfamiliar with national Cyber Security guidelines or basic digital protection procedures.

From the policy standpoint, enforcement and operationalization remain weak. Oyedapo and Akinlabi (2020) discovered that even when Cyber Security policies existed in some institutions, they were rarely enforced. Similarly, Uwaifo and Alabi (2022) emphasized that supportive government policy frameworks are essential to strengthen institutional security cultures. Cyber Security gaps also affect the end-user experience. Edewor and Osuchukwu (2020) found that poor information security undermines users' trust in digital library services. Obasuyi and Akporhonor (2019) concluded that low user awareness and weak authentication protocols increase susceptibility to cyber incidents.

Several studies highlight the need for holistic approaches. Omeluzor and Oyovwe-Tinuoye (2017) recommended the adoption of preservation mechanisms, secure authentication, and regular audits. Balogun and Adeyemi (2018) stressed the importance of combining technical solutions with behavioral change through staff training. Globally, Musa and Ibrahim (2023) noted that academic institutions with integrated Cyber Security frameworks experienced improved service

delivery and fewer breaches. Locally, Nwachukwu and Onuoha (2019) linked frequent cyber incidents in Nigerian libraries with poor contingency planning and budgetary constraints.

While literature on Cyber Security in southern Nigerian libraries is expanding, little empirical attention has been given to the North-East a region beset by socio-political instability and slower technological advancement. This study fills that gap by focusing on the Cyber Security measures, challenges, and service delivery implications for federal university libraries in the North-East.

## Method

This study adopted a descriptive survey research design to investigate Cyber Security measures and their influence on service delivery in federal university libraries in North East Nigeria. The population consisted of library and ICT staff from selected federal universities in the region, including the University of Maiduguri, Modibbo Adama University, Federal University of Technology Gombe, and Federal University Wukari. Using purposive sampling, four libraries with relatively advanced ICT infrastructures were chosen, and 60 respondents (15 from each university) were selected. Data were collected using a structured questionnaire titled *Cyber Security and Service Delivery Questionnaire (CSSDQ)*, which comprised both closed and open-ended items covering demographic data, Cyber Security practices, awareness levels, challenges, and service delivery impacts. The instrument's reliability was confirmed through a pilot study at a federal university outside the region, yielding a Cronbach Alpha of 0.82. The questionnaires were administered physically and electronically over four weeks, with necessary permissions obtained from university authorities. Collected data were analyzed using descriptive statistics (frequencies, percentages, and means) and Pearson correlation to examine the relationship between Cyber Security measures and service delivery, while qualitative responses were interpreted through thematic analysis to identify key patterns and insights.

## Results and Discussion

**Research Question 1:** What types of cyber security measures are currently available and implemented in federal university libraries in North East Nigeria?

**Table 1: Availability of Cyber Security Measures**

| Cyber security Tool/Measure | Libraries Using It (%) |
|---|---|
| Antivirus Software | 78 |
| Firewalls | 85 |
| Data Encryption Protocols | 18 |
| Intrusion Detection Systems | 22 |
| Formal Cyber security Policy | 45 |

The table shows that while antivirus software and firewalls are widely used (78% and 85% respectively), advanced cyber security tools like data encryption (18%) and intrusion detection systems (22%) are underutilized. Less than half (45%) of the libraries have a formal cyber security policy. This aligns with Eze & Uzoigwe (2022), who noted that many Nigerian academic libraries operate with basic protections while lacking comprehensive strategies. The absence of formal policy frameworks increases exposure to both internal and external threats.

**Research Question 2: To what extent are library staff and users aware of cyber security threats and preventive practices?**

**Table 2: Cyber security Training and Awareness**

| Cyber security Training Received | Frequency | Percentage (%) |
|---|---|---|
| Yes | 34 | 57 |
| No | 26 | 43 |
| Total | 60 | 100 |

Only 57% of respondents had received cyber security training, indicating moderate awareness levels. The remaining 43% lack basic cyber security literacy, which poses a significant

threat to digital asset safety. Ogunmodede & Akintola (2020) emphasized that untrained personnel are less likely to detect or respond appropriately to cyber threats, reinforcing the importance of regular training.

## Research Question 3: How effective are the existing cyber security measures in ensuring the integrity, confidentiality, and availability of digital library services?

**Table 3: E**ffectiveness of the existing cyber security measures

| Experience of Breach | Frequency | Percentage (%) |
|---|---|---|
| Yes | 36 | 60 |
| No | 24 | 40 |
| Total | 60 | 100 |

Despite the presence of basic measures, 60% of the libraries reported cyber security breaches in the past two years. This suggests limited effectiveness of current security implementations. The lack of advanced tools, staff training, and structured response plans undermines security efforts. As Babalola & Adebayo (2021) observed, reactive rather than proactive measures are common in academic libraries.

## Research Question 4: What are the major challenges facing the implementation of effective cyber security strategies in these libraries?

**Table 5: Major Challenges to Cyber security Implementation**

| Identified Challenge | Percentage of Respondents (%) |
|---|---|
| Inadequate Funding | 72 |
| Outdated ICT Infrastructure | 68 |
| Lack of Formal Cyber security Policy | 55 |
| Insufficient Staff Training | 43 |
| Limited Administrative Support | 40 |

| | |
|---|---|
| Low User Awareness | 35 |

The data above shows that the most frequently cited challenges were inadequate funding (72%) and outdated ICT infrastructure (68%), followed by lack of formal policy (55%) and poor staff training (43%). These challenges reflect structural weaknesses that restrict proactive security development. Similar barriers were highlighted by Okite-Amughoro et al. (2020), who observed that systemic neglect and underinvestment weaken cyber security readiness in academic institutions across Nigeria.

### Research Question 5: How do cyber security practices correlate with and impact the overall quality and efficiency of service delivery in federal university libraries in North East Nigeria?

**Table 4: Correlation between Cyber security Implementation and Service Delivery**

| Statistic | Value |
|---|---|
| Pearson Correlation Coefficient (r) | 0.68 |
| Significance Level (p) | < 0.05 |

A strong positive correlation ($r = 0.68$, $p < 0.05$) was found between the level of cyber security implementation and the efficiency of library services. This indicates that better cyber security is associated with fewer disruptions, greater user satisfaction, and more reliable digital access. Nwachukwu & Onuoha (2019) similarly reported that improved security enhances the academic utility of library systems.

### Research Question 6: What recommendations can be made to enhance cyber security and optimize service delivery in academic libraries within the region?

The study suggests: Development of formal cyber security policies; Investment in advanced tools (encryption, intrusion detection); Regular training programs for staff and users; Upgrading of ICT infrastructure, and Institutional and government funding support. These findings are supprted by Adebayo & Aina (2021), who advocated for strategic, multi-level approaches to cyber security improvement in Nigerian libraries.

**Recommendations**

Based on the findings of this study, the following recommendations are proposed to enhance Cyber Security measures and optimize service delivery in federal university libraries in North East Nigeria:

**1. Development of Comprehensive Cyber Security Policies:** It is critical for federal university libraries to implement formal Cyber Security policies. These policies should clearly outline roles, responsibilities, and procedures for managing Cyber Security risks, as well as define protocols for handling data breaches. Such policies will provide a structured approach to security management and help ensure consistency in practices across library systems.

**2. Investment in Advanced Cyber Security Technologies:** Libraries should prioritize investments in more advanced Cyber Security tools, including data encryption, intrusion detection systems, and secure authentication mechanisms. The implementation of these technologies will reduce the risk of cyber-attacks and enhance the security of sensitive academic and user data. Financial support from the university administration is crucial to achieve this.

**3. Regular Cyber Security Training and Awareness Programs:** Library staff and ICT personnel should undergo regular training to increase their awareness of Cyber Security threats and best practices for preventing security breaches. Training programs should cover topics such as phishing, malware prevention, secure use of library systems, and incident response. Additionally, user awareness programs should be organized for library patrons to help them understand how to protect their own data when accessing digital resources

**4. Strengthening ICT Infrastructure:** Universities in the North East should focus on upgrading and maintaining their ICT infrastructure to support the effective implementation of Cyber Security measures. This includes investing in modern hardware, reliable network systems, and backup solutions. Stronger infrastructure will support not only Cyber Security efforts but also improve overall service delivery to library users.

**5. Collaboration with External Cyber Security Experts:** Libraries can benefit from partnerships with Cyber Security experts and external agencies that specialize in academic Cyber Security solutions. External experts can assist in assessing the security needs of library systems, implementing advanced Cyber Security technologies, and conducting regular audits to identify and address vulnerabilities

**6. Increased Government and Institutional Support:** Government and university administrations should provide more financial and institutional support for Cyber Security initiatives in libraries. Given the increasing reliance on digital systems in academic institutions, funding for Cyber Security measures should be seen as an essential investment in the overall academic and research ecosystem. Additional support could include grants, subsidies, or budget allocations specifically for enhancing Cyber Security infrastructure.

**7. Establishing Incident Response and Recovery Plans:** Libraries should develop and regularly test incident response and recovery plans to minimize the damage caused by cyberattacks or system failures. These plans should include clear steps for identifying breaches, communicating with stakeholders, and recovering lost or compromised data. A robust recovery plan will ensure that library services can quickly return to normal after a Cyber Security incident, thereby minimizing disruptions to service delivery.

## Conclusion

This study has highlighted the crucial role of Cyber Security in ensuring the effective and secure delivery of library services in federal universities in North East Nigeria. While basic Cyber Security measures such as firewalls and antivirus software are in place, the study revealed

significant gaps in advanced security technologies, formal policies, and staff training. The frequent occurrence of Cyber Security breaches in the libraries, coupled with low levels of staff preparedness and insufficient institutional support, demonstrates the need for a comprehensive approach to Cyber Security.

The findings underscore that robust Cyber Security frameworks are not only necessary for protecting sensitive data but also for optimizing service delivery. Libraries with better Cyber Security practices reported higher user satisfaction and fewer disruptions in service, thus supporting the positive correlation between Cyber Security and service effectiveness. However, the challenges identified such as inadequate funding, outdated ICT infrastructure, and weak administrative commitment must be addressed to ensure sustainable improvements.

To enhance the overall security of digital resources and services in Nigerian academic libraries, especially in the North East, there is an urgent need for the development of comprehensive Cyber Security policies, the adoption of advanced technologies, and the implementation of regular training programs. By addressing these critical issues, federal university libraries can provide secure, reliable, and efficient services, fostering a more productive and safe academic environment.

## References

Abubakar, B. M., & Muhammad, A. (2021). Challenges of cybersecurity implementation in North-East Nigerian university libraries. *International Journal of Academic Library and Information Science*, 9(3), 28–36.

Adebayo, M. E., & Aina, R. F. (2021). Enhancing Library Services Through Cybersecurity Measures in Nigerian Academic Libraries. *Journal of Information Security Research*, 4(2), 34–45.

Ajegbomogun, F. O., & Salaam, M. O. (2019). Cybersecurity knowledge and practices among library staff in Nigerian universities. *Library Management*, 40(4/5), 273–286.

Azeez, A. L., & Oyelude, A. A. (2022). Security of digital library resources: Evidence from public universities in Nigeria. *African Journal of Library, Archives and Information Science*, 32(1), 1–15.

Balogun, T. A., & Adeyemi, A. M. (2018). Information systems security in Nigerian university libraries: A case study of three institutions. *Communicate: Journal of Library and Information Science*, 20(1), 15–25.

Babalola, Y. T., & Adebayo, M. E. (2021). Cybersecurity Awareness and Practices among Library Staff in Selected Nigerian University Libraries. *Journal of Library and Information Sciences*, 9(1), 45–58.

Edewor, N., & Osuchukwu, N. P. (2020). Users' perception of information security in digital library services. *Information Impact: Journal of Information and Knowledge Management*, 11(1), 67–79.

Eze, C. C., & Uzoigwe, C. U. (2022). Cyber Threats and the Security of Digital Information Resources in Nigerian Academic Libraries. *Library Philosophy and Practice*, Article 6612.

Musa, H. J., & Ibrahim, M. (2023). Evaluating the readiness of federal university libraries in Nigeria for digital threats. *International Journal of Library and Information Services*, 13(2), 61–74.

Nwachukwu, V. N., & Onuoha, J. (2019). Effects of Cybersecurity Breaches on Library Services in Nigerian Universities. *Nigerian Journal of Library and Information Science*, 16(1), 60–72.

Obasuyi, L. T., & Akporhonor, B. A. (2019). Security awareness and practices among library users in South-South Nigeria. *Nigerian Libraries*, 52(1), 80–91.

Ogunmodede, T. A., & Akintola, B. O. (2020). Evaluating Cybersecurity Literacy among Library Staff in Selected Public Universities in Nigeria. *African Journal of Library, Archives and Information Science*, 30(2), 159–168.

Okike, B. I. (2021). Digital security practices in academic libraries in Nigeria. *The Electronic Library*, 39(3), 435–451.

Okite-Amughoro, F. A., Okiy, R. B., & Ejikeme, A. N. (2020). Evaluation of ICT Utilization and Security Challenges in University Libraries in South-South Nigeria. *International Journal of Library and Information Science Studies*, 6(4), 1–16.

Omeluzor, S. U., & Oyovwe-Tinuoye, G. O. (2017). Digital preservation and information security in Nigerian university libraries. *Journal of Information Science Theory and Practice*, 5(2), 6–18.

Oyedapo, R. O., & Akinlabi, A. F. (2020). Analysis of ICT policies and their enforcement in Nigerian academic libraries. *Information Impact: Journal of Information and Knowledge Management*, 11(2), 45–59.

Tella, A., & Oguntayo, S. A. (2020). Staff attitude and institutional commitment to digital security in academic libraries. *Library Philosophy and Practice*, Article 4330.

Uwaifo, A. M., & Alabi, A. O. (2022). Role of government policy in strengthening cybersecurity in Nigerian universities. *Nigerian Journal of Library and Information Science*, 19(2), 91–105.

Uzoagba, I. N., & Echezona, R. I. (2021). Digital asset security strategies in Nigerian federal university libraries. *International Journal of Library and Information Technology*, 11(3), 23–37.

Yusuf, B. A., & Mohammed, S. A. (2022). Cybersecurity risk management in library systems: A proactive approach. *African Journal of Information Systems*, 14(1), 39–52.