



FUTIFMS International Conference

Data Privacy Awareness and Cybersecurity Practices in Academic Libraries: Implications for Digital Library Services in Nigerian Universities

Bola Christie Atulomah (PhD)

Federal University of Technology Ilaro.

Phone: 08034066694.

Email: bola.atulomah@federalpolyilaro.edu.ng

Abstract

The rapid digital transformation of academic libraries has enhanced access to information resources and strengthened support for teaching, learning, research, and scholarly communication. However, increasing reliance on digital technologies has intensified concerns regarding data privacy and cybersecurity. This review examines data privacy awareness, cybersecurity practices, and their implications for digital library services in Nigerian universities. Using a narrative review approach, relevant literature published between 2020 and 2026 was synthesized from scholarly databases, policy documents, and professional reports. Findings indicate that awareness of privacy and cybersecurity issues is growing among library professionals and users, yet significant challenges remain. These include inadequate funding, weak information and communication technology infrastructure, shortages of cybersecurity expertise, inconsistent policy implementation, evolving cyber threats, and difficulties associated with regulatory compliance. The review further reveals that effective privacy protection and cybersecurity practices enhance user trust, safeguard information assets, support service continuity, strengthen institutional reputation, and promote sustainable digital library services. The study concludes that data privacy awareness and cybersecurity have become indispensable components of modern academic library management. Strengthening awareness programmes, governance frameworks, technological infrastructure, professional competencies, and regulatory compliance will improve the resilience and sustainability of digital library services in Nigerian universities.

Keywords: Data Privacy, Academic Libraries, Cybersecurity, Digital Library Services, Data Protection, Nigerian Universities

Introduction

The advancement of information and communication technologies has transformed academic libraries from primarily physical repositories into digital information environments that support teaching, learning, research, and scholarly communication (Tawil & Miao, 2024; Borgman, 2025). Through electronic databases, institutional repositories, cloud-based services, and digital archives, libraries now provide broader and more efficient access to information resources.

While digital transformation has improved service delivery, it has also increased exposure to privacy and cybersecurity risks. Academic libraries manage significant volumes of personal, institutional, and research-related information, making them attractive targets for cybercriminals. Threats such as phishing attacks, ransomware, malware infections, unauthorized access, and data breaches have become major concerns for higher education institutions (Igbinovia et al., 2026).

In Nigeria, the adoption of digital library services has expanded considerably over the last decade. However, concerns persist regarding cybersecurity preparedness, privacy governance, technological infrastructure, and compliance with the Nigeria Data Protection Act (NDPA) 2023. Despite growing scholarly interest in cybersecurity and information management, relatively few studies have examined the combined influence of data privacy awareness and cybersecurity practices on digital library services within Nigerian universities. This review addresses that gap by synthesizing existing literature and examining implications for sustainable digital library development.

Statement of the Problem

The increasing adoption of digital technologies has transformed academic libraries into sophisticated digital information environments, improving access to electronic resources,

institutional repositories, and online library services. However, this transformation has also exposed academic libraries to growing cybersecurity threats and data privacy risks. Recent studies indicate that higher education institutions are increasingly targeted by cyberattacks such as phishing, ransomware, malware, data breaches, and unauthorized access, which threaten the confidentiality, integrity, and availability of digital information resources (Lallie et al., 2023; Salam et al., 2026). These incidents have raised concerns about the ability of academic libraries to safeguard users' personal information and maintain trust in digital library services.

Despite growing awareness of cybersecurity and data privacy, evidence suggests that many academic libraries, particularly in developing countries, continue to face significant implementation challenges. Studies have identified inadequate funding, obsolete ICT infrastructure, shortages of cybersecurity professionals, weak governance structures, and inconsistent compliance with data protection regulations as major barriers to effective cybersecurity management (Udumukwu & Nwali, 2024; Asere et al., 2025). Similarly, Musa and Yelwa (2025) reported persistent data privacy and security challenges in digital libraries of tertiary institutions, highlighting deficiencies in institutional preparedness and user awareness.

Although previous studies have examined data privacy, cybersecurity, and digital library services independently, limited attention has been given to their combined influence on the effectiveness and sustainability of digital library services in Nigerian universities. Furthermore, there is a paucity of review studies synthesizing recent evidence following the enactment of the Nigeria Data Protection Act (NDPA) 2023. This gap limits a comprehensive understanding of emerging cybersecurity practices, privacy awareness, regulatory compliance, and their implications for digital library service delivery. Therefore, this study undertakes a narrative review to synthesize current literature on data privacy awareness and cybersecurity practices

and to examine their implications for sustainable digital library services in Nigerian universities.

Objectives of the Study

This paper seeks to:

1. examine the level of data privacy awareness in academic libraries;
2. identify cybersecurity practices adopted in academic libraries;
3. explore challenges associated with privacy protection and cybersecurity in Nigerian university libraries; and
4. discuss the implications of data privacy and cybersecurity for sustainable digital library services.

Research Questions

1. what is the level of data privacy awareness in academic libraries;
2. What are the cybersecurity practices adopted in academic libraries;
3. What are the challenges associated with privacy protection and cybersecurity in Nigerian university libraries; and
4. What are the implications of data privacy and cybersecurity for sustainable digital library services.

Conceptual and Theoretical Perspectives

Data privacy refers to the protection of personal information from unauthorized access, use, disclosure, modification, or destruction, while cybersecurity encompasses the technologies, policies, and practices used to safeguard information systems and digital assets (Akinyede et

al., 2021; Asere et al., 2025). Although distinct, both concepts are interdependent. Effective privacy protection requires adequate cybersecurity measures, while cybersecurity initiatives help preserve confidentiality and integrity of personal information.

This review is informed by three complementary theoretical perspectives. Information Security Awareness Theory emphasizes the importance of user knowledge and awareness in reducing security vulnerabilities (Bulgurcu et al., 2010). Protection Motivation Theory explains how perceptions of threats and confidence in protective measures influence security behavior (Rogers, 1975). The Technology Acceptance Model highlights the role of perceived usefulness and ease of use in the adoption of cybersecurity technologies (Davis, 1989). Together, these theories suggest that awareness, motivation, and technology acceptance are essential for effective cybersecurity and privacy protection within academic libraries.

Thematic Review of Literature

The literature consistently identifies data privacy awareness as a critical factor in protecting digital library environments. Academic libraries routinely manage user registration records, borrowing histories, search activities, authentication credentials, and research outputs. Consequently, librarians and information professionals require adequate understanding of privacy principles, ethical responsibilities, and regulatory obligations. Although awareness has improved, studies indicate that knowledge levels remain uneven across institutions, limiting effective privacy governance and compliance (Saha, 2024).

Cybersecurity awareness among library users is equally important. Students, researchers, faculty members, and administrators increasingly depend on digital information systems and remote access platforms. Human behavior remains one of the most significant contributors to cybersecurity incidents, as many attacks exploit user vulnerabilities rather than technical weaknesses. Weak passwords, credential sharing, phishing susceptibility, and unsafe online

practices continue to expose institutions to significant risks (Musa & Yelwa, 2025; Parsons et al., 2014).

The literature further demonstrates that academic libraries face a diverse and evolving cybersecurity threat landscape. Common threats include phishing attacks, malware infections, ransomware incidents, identity theft, insider threats, data breaches, cloud security vulnerabilities, and emerging artificial intelligence-related risks (Lallie et al., 2023; Salam et al., 2026). These threats have the potential to compromise the confidentiality, integrity, and availability of digital library resources while disrupting teaching, learning, and research activities.

To address these risks, academic libraries increasingly adopt cybersecurity practices such as password management, access controls, multi-factor authentication, encryption, software updates, backup systems, security awareness programmes, network protection measures, and incident response planning (Johnson, 2020; Currier, 2021). Effective cybersecurity depends not only on technological safeguards but also on governance frameworks, policy implementation, and continuous user education.

Despite these efforts, Nigerian academic libraries continue to face substantial challenges. Inadequate funding remains a major barrier to investment in cybersecurity technologies and infrastructure. Many institutions operate with outdated hardware, limited bandwidth, unstable internet connectivity, and unreliable power supply. Additional challenges include shortages of cybersecurity professionals, weak governance structures, insufficient awareness programmes, and difficulties complying with regulatory requirements such as the NDPA 2023 (Udumukwu & Nwali, 2024; Salam et al., 2026).

The literature emphasizes that sustainable cybersecurity requires an integrated approach combining technology, policy, awareness, governance, and professional capacity development.

Institutions that successfully integrate these components are better positioned to protect digital resources, maintain service continuity, and strengthen user trust.

Gaps in the Literature

Several important gaps remain within existing scholarships. First, data privacy awareness and cybersecurity practices are frequently examined independently, resulting in limited understanding of their combined influence on digital library effectiveness. Second, many studies focus on universities broadly rather than academic libraries as unique digital information environments.

The literature also reveals a predominance of descriptive studies, with limited longitudinal and comparative research examining cybersecurity maturity, privacy governance, and service outcomes over time. Furthermore, relatively little empirical evidence directly links cybersecurity practices to user trust, service utilization, research productivity, and digital library sustainability.

Research addressing implementation of the Nigeria Data Protection Act (NDPA) 2023 within academic libraries remains limited. Similarly, insufficient attention has been devoted to emerging technologies such as artificial intelligence, cloud computing, and advanced analytics despite their growing influence on digital library operations.

Implications for Digital Library Services

The findings have important implications for digital library services in Nigerian universities. Effective privacy protection and cybersecurity practices contribute significantly to user trust and confidence. Users are more likely to engage with digital resources when they believe their personal information is adequately protected.

Strong cybersecurity measures also protect institutional information assets, preserve research integrity, and support service continuity. Cybersecurity incidents can disrupt access to critical resources, undermine institutional reputation, and negatively affect teaching, learning, and research activities.

The evolving digital environment further expands the educational role of academic libraries. Beyond providing information resources, libraries are increasingly expected to promote cybersecurity literacy, privacy awareness, and responsible digital citizenship. Consequently, privacy protection and cybersecurity should be viewed as strategic components of digital transformation and sustainable library development.

Conclusion

Data privacy awareness and cybersecurity have become essential components of academic library management in the digital era. As Nigerian universities continue to expand digital library services, the protection of personal information and institutional resources must remain a strategic priority. Although awareness and cybersecurity practices have improved, significant challenges relating to infrastructure, funding, expertise, governance, and compliance persist. The evidence reviewed demonstrates that effective privacy protection and cybersecurity management enhances user trust, strengthens service resilience, supports regulatory compliance, and contributes to the long-term sustainability of digital library services. An integrated approach combining technology, policy, governance, education, and professional development is therefore essential for building secure, reliable, and future-ready academic library environments in Nigerian universities.

Recommendations

Several measures are necessary to strengthen cybersecurity and privacy protection within Nigerian academic libraries.

1. Continuous privacy and cybersecurity awareness programmes should be implemented for librarians and users.
2. Universities should develop and enforce comprehensive cybersecurity policies aligned with the Nigeria Data Protection Act (NDPA) 2023.
3. Greater investment is required in secure ICT infrastructure, backup systems, and cybersecurity technologies.
4. Academic libraries should strengthen professional capacity through specialized cybersecurity training and development programmes.
5. Regular security audits, risk assessments, and incident response planning should become standard institutional practices.
6. Collaboration among libraries, regulatory agencies, professional bodies, and information technology units should be strengthened to promote information security best practices.

References

- Adediran, O. & Okon, I. (2023). "Challenges of data privacy enforcement in Nigeria: A regulatory perspective". *Journal of Cybersecurity and Data Protection*. 5(2): 45-62
- Akinyede, O.; Awodele, O. & Agbeyangi, A. (2021). "Awareness and compliance with Nigeria Data Protection Regulation among Nigerian organizations". *Journal of Cyber Security Technology*. 5(2): 140-159. <https://doi.org/10.1080/23742917.2021.1902094>
- Anderson, R., Evans, G., & Ensor, J. (2025). Cybersecurity in the library: Steps you can take now to make your users and your institutions safer. *Proceedings of the IATUL Conferences*. Purdue University Libraries. <https://docs.lib.purdue.edu/iatul/2024/edi/1/>
- Aregbesola, A., & Nwaolise, E. L. (2023). Securing digital collections: Cyber security best practices for academic libraries in developing countries. *Library Philosophy and Practice (e-journal)*, 7822. <https://digitalcommons.unl.edu/libphilprac/7822/>.
- Asere, G. F., Adenomon, M. O., Aimufua, G. I. O., & Ibrahim, U. (2025). The effects of data privacy regulations on cybersecurity practices in Nigeria and Africa. *Cyberspace Studies*, 9(2), 313–336. <https://doi.org/10.22059/jcss.2025.390087.1127>.
- Borgman, C. L. (2025). Libraries, digital libraries, and data: Forty years, four challenges. *arXiv*. <https://arxiv.org/abs/2506.15055>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/2575069>
- Currier, C. (2021). Unresolved privacy and ethics issues related to learning analytics in higher education and academic librarianship. *Emerging Library & Information Perspectives*, 4, 117–142. <https://doi.org/10.5206/elif.v4i1.13463>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- Federal Republic of Nigeria. (2023). Nigeria Data Protection Act, 2023. Government of Nigeria. <https://ndpc.gov.ng/>
- Igbinovia, M. O., Osawaru, K. E., Onaivi, E. N., Baipe, E. O., Akidi, J. O., & Aiyebelehin, A. J. (2026). Cyber threats to libraries and the implications for the actualization of the sustainable development goals: A narrative review. *Southern African Journal of Security*. Advance online publication. <https://doi.org/10.25159/3005-4222/19016>
- International Federation of Library Associations and Institutions. (2015). IFLA statement on privacy in the library environment. International Federation of Library Associations and Institutions. <https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment/>
- Johnson, Q. (2020). Privacy considerations for library and information professionals. *Information Services & Use*, 40(3), 233–239. <https://doi.org/10.3233/ISU-200089>
- Kim, B. (n.d.). Keeping up with... Cybersecurity, usability, and privacy. Association of College and Research Libraries. https://www.ala.org/acrl/publications/keeping_up_with/cybersecurity

- Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). Understanding cyber threats against universities, colleges, and schools. *arXiv Preprint*. <https://arxiv.org/abs/2307.07755>
- Musa, H., & Yelwa, A. S. (2025). Data privacy and security challenges in digital libraries of tertiary institutions in Zamfara State. *FUGUS International Journal of Library and Information Science*, 2(2), 79–89. <https://doi.org/10.57233/fijlis.v2i2.08>
- Nigeria Data Protection Commission. (2023). *Nigeria Data Protection Act (NDPA), 2023*. Federal Republic of Nigeria.
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Saha, R. (2024). Data privacy and cyber security in digital library perspective: Safeguarding user information. *International Journal of Scientific Research in Engineering and Management (IJSREM)*, 8(4), 1–5. <https://doi.org/10.55041/IJSREM30761>
- Salam, M., Abu Bakar, K. A., Ghani, A. T. A., & Aman, A. H. M. (2026). Cybersecurity in higher education institutions digitalisation: Addressing threats and vulnerabilities. *SAGE Open*, 16(1). <https://doi.org/10.1177/21582440251413473>.
- Tawil, S., & Miao, F. (2024). Steering the digital transformation of education: UNESCO's human-centered approach. *Frontiers of Digital Education*, 1(1), 51–58. <https://doi.org/10.1007/s44366-024-0020-0>.
- Udumukwu, I. J., & Nwali, V. C. (2024). Cybersecurity and privacy in federal university libraries in Nigeria. *Journal of Applied Information Science and Technology*, 17(2), 107–117.