IJoL International Journal of Librarianship

ISSN: 2474-3542 Journal homepage: https://journal.calaijol.org

Nigerian Library and Information Science Curriculum Modification: The Need for Cybersecurity Inclusion Through a Narrative Literature Review Methodology

Adeyinka Tella

Abstract:

The evolving digital landscape and the rise in cyber threats necessitate a strategic reassessment of the Nigerian Library and Information Science (LIS) curriculum. This study employs a narrative literature review methodology to explore the imperative of integrating cybersecurity education into LIS programs in Nigeria. The review synthesizes relevant academic and grey literature to identify existing gaps in LIS curricula, assess international trends, and highlight competencies required by modern information professionals in safeguarding digital assets. Findings indicate that current LIS training in Nigeria largely overlooks cybersecurity, despite increasing digitization of library services and data-driven operations. The review underscores the need to equip LIS graduates with fundamental cybersecurity knowledge, including data protection, digital ethics, cyber hygiene, and information assurance. It also reveals global best practices where LIS schools have successfully embedded cybersecurity modules into core programs. The study concludes by recommending collaborative efforts among academic institutions, policymakers, and professional bodies to reform LIS education in Nigeria, ensuring relevance in a technology-centric world. Integrating cybersecurity into LIS curricula will not only enhance graduates' employability but also strengthen the resilience and credibility of information institutions in Nigeria.

To cite this article:

Tella, A. (2026). Nigerian Library and Information Science Curriculum Modification: The Need for Cybersecurity Inclusion Through a Narrative Literature Review Methodology. *International Journal of Librarianship*, *11*(3), 88-131. https://doi.org/10.23974/ijol.2026.vol11.3.646

To submit your article to this journal:
Go to https://ojs.calaijol.org/index.php/ijol/about/submissions

INTERNATIONAL JOURNAL OF LIBRARIANSHIP, 11(3), 88-131
ISSN: 2474-3542

Nigerian Library and Information Science Curriculum Modification: The Need for Cybersecurity Inclusion Through a Narrative Literature Review Methodology

Adeyinka Tella
University of Ilorin, Nigeria, and
University of South Africa, Pretoria, South Africa

ABSTRACT

The evolving digital landscape and the rise in cyber threats necessitate a strategic reassessment of the Nigerian Library and Information Science (LIS) curriculum. This study employs a narrative literature review methodology to explore the imperative of integrating cybersecurity education into LIS programs in Nigeria. The review synthesizes relevant academic and grey literature to identify existing gaps in LIS curricula, assess international trends, and highlight competencies required by modern information professionals in safeguarding digital assets. Findings indicate that current LIS training in Nigeria largely overlooks cybersecurity, despite increasing digitization of library services and data-driven operations. The review underscores the need to equip LIS graduates with fundamental cybersecurity knowledge, including data protection, digital ethics, cyber hygiene, and information assurance. It also reveals global best practices where LIS schools have successfully embedded cybersecurity modules into core programs. The study concludes by recommending collaborative efforts among academic institutions, policymakers, and professional bodies to reform LIS education in Nigeria, ensuring relevance in a technology-centric world. Integrating cybersecurity into LIS curricula will not only enhance graduates' employability but also strengthen the resilience and credibility of information institutions in Nigeria.

Keywords: Cybersecurity, Library and Information Science (LIS), Curriculum Development, Nigerian LIS Education, Narative Review, Digital Literacy, Information Security, LIS Reform, Cyber Threats, ICT Integration

INTRODUCTION

The scope and functions of libraries and information centers have changed as a result of the global acceleration of digital transformation. Academic, public, and special libraries in Nigeria are depending more and more on information and communication technologies (ICTs) to support user services, manage collections, and make information easier to access. Although there are many advantages to this digital transformation, libraries are now at risk from serious cybersecurity risks such as ransomware attacks, data breaches, and digital vandalism (Ahmed & Ahmed, 2024). Nigerian Library and Information Science (LIS) programs urgently need to update their curricula to include cybersecurity instruction and skill development in light of these issues.

The issue of cybersecurity is no longer limited to technical occupations. Information professionals now play a crucial role in maintaining information security since they are the keepers of private, institutional, and occasionally classified data (Chaudhary et al., 2023). The International Federation of Library Associations and Institutions (IFLA) emphasizes that protecting information integrity and confidentiality in a digital setting is a professional and ethical obligation of LIS professionals (IFLA, 2015; Omoike & Alabi, 2023). Because of this, LIS workers need to have the knowledge and abilities needed to handle information assets safely. However, the majority of LIS programs in Nigeria continue to follow conventional curricula with little regard for digital risk management and information security (Abubakar, 2021). The absence of organized and context-specific cybersecurity information is a significant weakness in Nigeria's existing LIS curriculum. Nigerian LIS graduates are frequently unprepared to handle or react to changing digital dangers within information environment, in contrast to their colleagues in more developed nations (Ezema et al., 2023; Dunmade & Tella, 2023). The professional relevance and adaptability of LIS education in the face of the worldwide digital transformation are called into question by this curriculum lag. Inadequate cybersecurity training compromises libraries' larger purpose as reliable resources for information access and preservation in addition to having an impact on the performance and reputation of LIS graduates.

In order to incorporate new multidisciplinary fields like data science, artificial intelligence, computational archives, quantum information management, quantum information retrieval, quantum cryptography and information security, and cybersecurity, LIS education is changing globally (Pinki, 2024). For future professionals to be able to adopt strong digital practices, respect information ethics, and make a significant contribution to organizational and national information security goals, cybersecurity must be incorporated into LIS curricula. This change presents both a strategic opportunity and a requirement in the Nigerian setting. There is a strong need for curriculum change given the rise in cybercrime occurrences in the nation, which includes attacks on government and educational institutions (Igwe, 2021).

Despite the necessity, there isn't much comprehensive research that outlines the current status of LIS curricula in Nigeria with regard to cybersecurity. This study fills that gap by investigating the degree of cybersecurity representation in Nigerian LIS curricula through a systematic literature review. In domains where new subjects necessitate a thorough, exploratory mapping of current knowledge and practice, narrative reviews are especially helpful (Mak & Thomas, 2022). The study provides a basis for additional empirical research and policy interventions by identifying important themes, gaps, and potential for incorporating cybersecurity into LIS curriculum through this methodology. This study's main objective is to provide well-informed suggestions that can help LIS instructors, curriculum developers, regulatory agencies, and legislators include cybersecurity into LIS curricula. By doing this, the study helps Nigeria's attempts to create a knowledge society that is secure and robust in the face of digital change while also adding to the larger conversation on digital transformation in library education. Giving LIS workers cybersecurity skills is not just an academic improvement; it is a national necessity as the information management landscape changes.

Library and information science (LIS) must constantly change to be relevant in a time of fast digital revolution. Libraries all over the world are increasingly digitally-driven knowledge

centers rather than traditional, physical information stores. This development has had a big impact on how LIS is taught and used in Nigeria. But even with these developments, there is still a significant gap in the nation's LIS curriculum: cybersecurity is not given enough attention. Libraries are more vulnerable to cyberattacks as they use information and communication technologies (ICT) more and more. Therefore, it is not only appropriate but also crucial to incorporate cybersecurity instruction into the LIS curriculum. This study, employing a narrative literature review methodology, explores the trajectory of LIS education in Nigeria, its adaptation to technological changes, and the urgent need for cybersecurity inclusion.

BRIEF HISTORY OF LIS EDUCATION IN NIGERIA

The introduction of certificate and diploma programs in the 1950s, during the colonial era, to prepare librarians for employment in academic and public libraries marked the official beginning of LIS education in Nigeria. In the early 1960s, the University of Ibadan was the first to offer library science programs at the degree level. Other universities including Ahmadu Bello University and the University of Nigeria, Nsukka, followed suit. These curricula, which placed a strong emphasis on cataloguing, categorization, reference services, and library management, were mostly based on American and British LIS education systems. The administration of print-based collections, bibliographic control, and manual information retrieval were the initial foundations of LIS training. But as the field developed, new fields were added, like documentation, archiving, and records management. However, ICT and digital literacy, which would only start to play a significant role in the 2000s, were not well-represented in the early curricula.

Visual Aid 1: Timeline Diagram

Fig 1 is a timeline showing major milestones in Nigerian LIS education from colonial-era training programs to the establishment of ICT-based modules in the early 2000s would contextualize this evolution effectively.

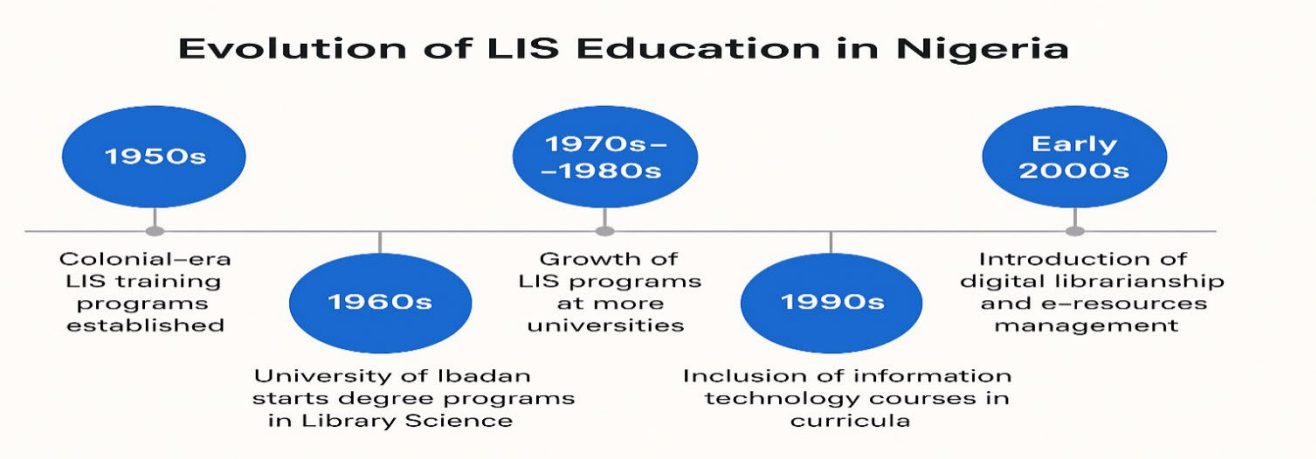


Fig 1: Evolution of Education in Nigeria

The Evolution of LIS Curriculum Vis-à-vis Technological Changes

Nigerian libraries started implementing internet access platforms, digitized archives, and Integrated Library Management Systems (ILMS) as a result of the 21st century's boom of digital technology. As a result, LIS departments were forced to update their courses to take into account the evolving nature of information work. To give students the skills they need for the digital world, modules including information technology, digital librarianship, metadata, and e-resources management were included. The rate of curricular reform has not kept up with the growing complexity of the digital information environment, notwithstanding these revisions. The majority of Nigerian LIS programs lack courses that specifically address data protection, cyber hygiene, ethical hacking, digital forensics, or information assurance (Familoni & Shoetan, 2024). The potential of security breaches in library systems is becoming a greater concern as information becomes more valuable and fragile, which emphasizes how crucial cybersecurity expertise is for LIS personnel.

Visual Aid 2: Infographic

An infographic contrasting traditional LIS skills (e.g., cataloguing, indexing, bibliographic instruction) with modern LIS skillsets (e.g., data analytics, digital preservation, cybersecurity awareness) would visually capture the skill transition required for today's professionals (see fig 2):

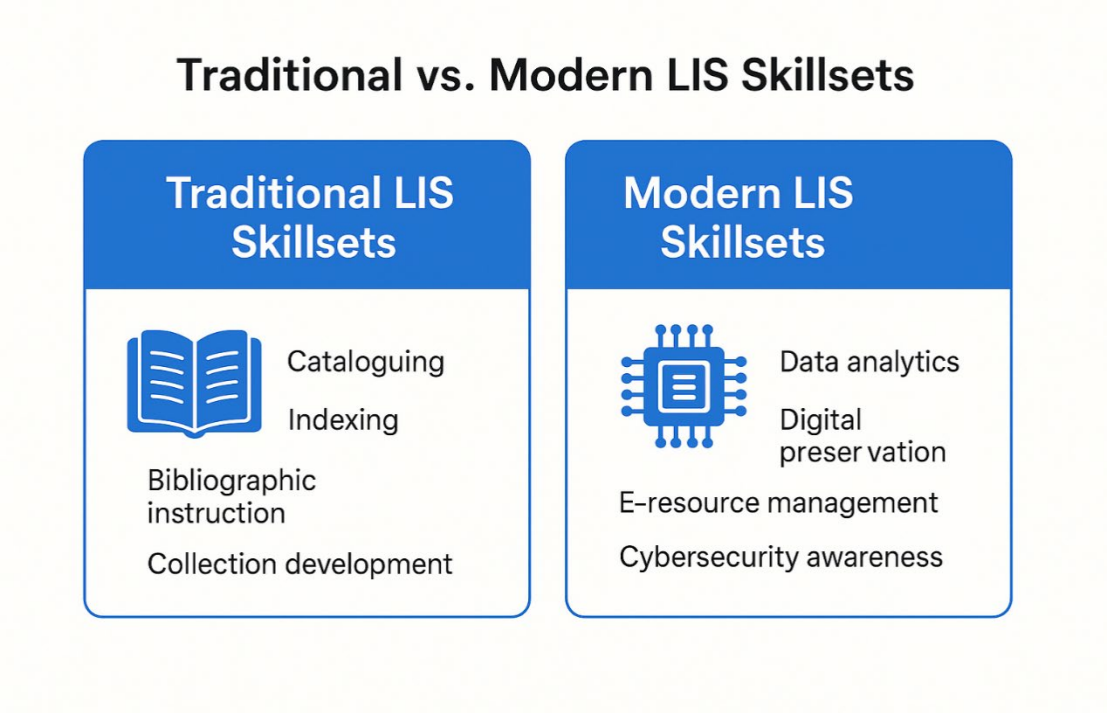


Fig 2: Traditional and Modern LIS Skillsets

The Essentiality of Cybersecurity in Information Professions

Nowadays, cybersecurity is a fundamental skill for information workers everywhere. Large amounts of sensitive data, including as user identities, borrowing histories, academic records, and even intellectual property, are handled by libraries, academic institutions, archives, and documentation centers (Saha, 2024). Cyberattacks on public and educational institutions have increased in frequency in Nigeria, highlighting the weaknesses in digital infrastructures. LIS specialists are frequently at the forefront of user data and digital resource management (Ebelogu et al., 2025). They run the danger of unintentionally enabling breaches through poor digital hygiene or ignorance of threat mitigation if they don't receive enough cybersecurity training. The need for LIS graduates to be prepared to handle these difficulties is increasing as libraries transform into digital information hubs and Nigeria moves closer to becoming a more digital society through programs like the National Digital Economy Policy and Strategy (2020–2030). By including cybersecurity into LIS courses, professionals are better equipped to safeguard information assets and establish themselves as essential contributors to the nation's digital resilience. When such competencies are absent from a curriculum, a serious vulnerability goes unchecked.

Rationale for Cybersecurity in LIS Education

There is a pressing need to reconsider the design and content of Library and Information Science (LIS) education in light of the increasing interdependence of technology and library services in the digital age, particularly in light of Society 5.0. As libraries in Nigeria undergo substantial digitization, protecting library information systems from growing cyberthreats becomes especially important. Not only is integrating cybersecurity education within the LIS curriculum an academic innovation, but it is also an essential response to the ethical, social, and technological issues of the real world. Three interconnected factors can be used to discuss the case for cybersecurity inclusion: the expanding digitization of library services, the expansion of cyberthreats directed at libraries, and the crucial role that libraries play as guardians of private user information. LIS practice has changed from manual systems to highly automated, networked, and cloud-based digital environments in Nigeria and around the world. Online Public Access Catalogs (OPACs), digital repositories, integrated library systems (ILS), and mobile-accessible library platforms have replaced traditional card catalogs (Wells, 2021; Bakrin et al., 2020). In addition to greatly improving user experience and information availability, this digital revolution has also greatly increased the attack surface for cybercriminals.

Nigerian libraries, especially academic, public, and special libraries, may now provide remote access to scholarly databases, e-journals, e-books, and institutional repositories thanks to digitization efforts (Adejumo et al., 2015). The complexity of library operations has further expanded with the increasing integration of technology like digital lending platforms, RFID (Radio Frequency Identification) systems, and AI-powered information retrieval systems. Professional LIS practitioners who are competent cybersecurity stewards in addition to information managers are needed as a result of our growing dependency on ICT infrastructure (Singh et al., 2025; Idhalama et al., 2025). Many LIS programs in Nigeria have yet to include formal cybersecurity training in their curricula, despite the advancements in digitization (Jegbefume et al., 2025). Future librarians are ill-prepared for the ethical, legal, and technological ramifications of handling user

data and digital collections in a potentially hostile cyber environment because of this gap. LIS education must give students the skills they need to foresee, stop, and address cybersecurity threats as digital services grow (Ismail et al., 2025). Libraries are being viewed as active hubs in the digital information economy rather than just passive book repositories. As a result, malevolent cyber actors are increasingly targeting them. The threats facing library information systems are diverse and evolving, ranging from phishing attacks and data breaches to ransomware, denial-of-service (DoS) attacks, and insider threats (Singh et al., 2025).

Data Breaches: Large volumes of user data, such as contact details, borrowing histories, interlibrary loan requests, and occasionally even biometric information for identification, are gathered and maintained by libraries. Unauthorized access to this data may result in surveillance, identity theft, or harm to one's reputation (D'Amato, 2025). Libraries in Nigeria are especially susceptible to breaches due to inadequate cybersecurity infrastructure and legislative gaps, particularly in cases where systems are not routinely updated or monitored (Alliance Law Firm, ALF, 2025).

Ransomware Attacks: Ransomware has become a serious danger to public institutions, especially libraries, in recent years. Critical files are encrypted by cybercriminals, who then demand payment to unlock them, so stopping library services. If targeted, a Nigerian academic library lacking sufficient backup systems and skilled personnel may experience operational paralysis, which would impact student learning results as well as the institution's ability to conduct research (Sahabi & Otobo, 2021).

Digital Vandalism and Data Manipulation: Library public access terminals, particularly those in underprivileged areas, are frequently susceptible to malware or improper use. Attackers can insert dangerous programs into open access materials, change digital resources, or deface websites. This makes library platforms less reliable and puts patrons at even greater risk (Okusi, 2024).

Negligence and Insider Threats: Without sufficient cybersecurity knowledge, librarians and IT support personnel run the risk of unintentionally compromising systems. Attacks may be made possible by using weak passwords, storing data in an unprotected manner, or delaying updates. If not adequately taught, the Nigerian LIS workers can unintentionally increase the cyber vulnerability of their organization (Agwu-Okoro, 2025).

Together, these dangers show why cybersecurity cannot be handled solely by the IT department and needs to be incorporated into LIS practice and instruction. LIS graduates will be more equipped to evaluate risk, implement data protection procedures, and work with technical teams to create reliable information systems if they integrate cybersecurity principles (Abrahams et al., 2024). Libraries naturally promote privacy and intellectual independence. In order to measure resource usage, personalize services, and enhance operations, they gather and handle sensitive user data. According to Ikwuanusi et al. (2023), this includes user profiles, search histories, borrowing patterns, and even interaction logs from chat-based or AI-assisted reference services. In some digital library platforms, integration with institutional portals means that academic libraries may handle course enrollments, grades, or staff employment data.

The ethical duty of librarians to safeguard privacy becomes crucial in Nigeria, where there is a disparity in digital literacy and consumers may not be aware of their rights or the consequences of data misuse. Without proper training, librarians might unintentionally disregard global standards like the General Data Protection Regulation (GDPR) or Nigeria's Data Protection Act (NDPA, 2023 Chukwumaobi, 2018) by neglecting to apply access controls, anonymize data, or keep consent records (One Trust DataGuide, 2020; Weitzenboeck et al., 2022; George, 2025). Furthermore, when patrons steer clear of digital services due to privacy concerns or a fear of surveillance, libraries' fundamental role of promoting fair access is compromised. Users must have faith that their information is shielded from abuse, monitoring, or unapproved sharing if libraries are to continue to be secure places for study and inquiry (Popoola et al., 2023). Trust must be gained via open policies and safe infrastructure; it cannot be taken for granted. Given this, LIS education in Nigeria has to prioritize user advocacy, data governance, and ethical literacy in addition to technical cybersecurity abilities. A librarian who is knowledgeable about cybersecurity will be able to advocate for user rights, apply privacy-by-design principles to library systems, and react effectively to data incidents (Igbinovia & Clifford, 2023; Ocks & Salubi, 2024).

It is now academically and professionally necessary for cybersecurity to be taught in Nigerian LIS programs; it is no longer an elective. Managing secure information systems becomes more complicated and riskier as library services become more digitalized. Data breaches, ransomware, and insider threats are just a few of the many cyberthreats that LIS professionals need to be prepared to recognize and handle. The ethical obligation to protect the data and privacy of various user populations is equally significant, especially in a developing country like Nigeria where security knowledge and digital trust are still growing. The profession will remain robust, relevant, and morally grounded in the face of 21st-century issues if the LIS curriculum is revised to incorporate cybersecurity ideas ranging from fundamental digital hygiene to sophisticated threat response methods. Those in charge of libraries must be well equipped to protect their digital frontiers as they remain digital entry points to knowledge and opportunity. Figure 3 shows some of the common cybersecurity issues they should be aware of.

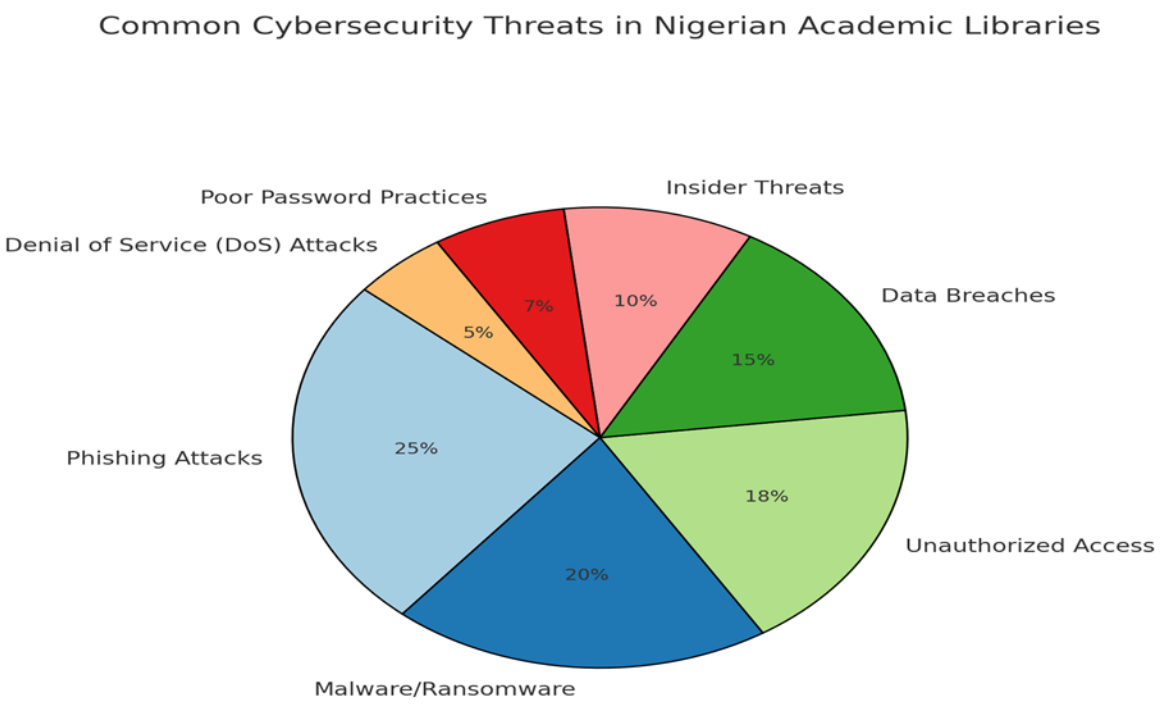


Fig 3: Common cybersecurity threats in Nigerian academic libraries

Table 1: Interpretation of the Pie Chart: Common Cybersecurity Threats

Threat	Percentage	Interpretation
Phishing Attacks	**25%**	Phishing is the most prevalent threat, making up a quarter of the cybersecurity risks. Attackers often impersonate trusted sources (like university portals, library staff, or email systems) to trick users especially staff and students into revealing sensitive credentials or clicking malicious links. This high percentage signals a critical need for regular awareness training and simulated phishing campaigns.
Malware/Ransomware	**20%**	Malware and ransomware infections account for one-fifth of threats. These often result from downloading infected e-resources, visiting compromised websites, or using unsecured USB drives. In libraries with outdated systems or poor antivirus defenses, ransomware can encrypt important academic or user data, making it inaccessible unless a ransom is paid.
Unauthorized Access	**18%**	Unauthorized access occurs when users (internal or external) gain entry to restricted systems or data often due to weak passwords, shared credentials, or poor user access management. At 18%, this points to the need for identity and access management (IAM) systems and enforcing role-based permissions.
Data Breaches	**15%**	Breaches where sensitive user data is leaked or stolen are responsible for 15% of the threat landscape. In academic libraries, this can involve exposure of student information, research materials, login details, or licensing data. Causes range from poor encryption to server misconfigurations and outdated software.
Insider Threats	**10%**	These stem from individuals within the institution staff or students who intentionally or unintentionally compromise security. It could be a disgruntled staff member leaking records, or a student misusing access. This threat highlights the need for user behavior monitoring, data access logs, and staff screening policies.
Poor Password Practices	**7%**	Weak, reused, or shared passwords expose systems to brute-force and credential-stuffing attacks. This figure suggests that while not the top threat, password misuse still undermines institutional cybersecurity. A policy enforcing strong password creation and periodic changes is vital.
Denial of Service (DoS)	**5%**	Though the least frequent, DoS attacks can still cause significant disruptions. In this context, attackers may flood library servers, online catalogs, or e-resource portals to make them unavailable, particularly during peak academic

Threat	Percentage	Interpretation
		periods. Libraries need firewalls and rate-limiting defenses to mitigate such attacks.

Together, the top three threats phishing (25%), malware (20%), and unauthorized access (18%) represent 63% of the total, demonstrating the dominance of technological exploits and social engineering. The significance of human-centric security methods is emphasized by the behavioral character of lower but still significant concerns like insider threats and password problems. Even though DoS is at its lowest, it can nevertheless paralyze library systems when they are needed for important tasks like exams, journal access online, or e-library use.

Image of a breached library database interface for visual impact

Figure 4 serves as a visual alert that a library database has been breached, which means that private material has been accessed or perhaps stolen by unauthorized parties. Below is a summary of the essential components:

A critical and urgent emergency is indicated by the bold red "ALERT" at the top.

The text "LIBRARY DATABASE COMPROMISED" makes it obvious that a library's digital system security has been compromised.

An exclamation points and padlock on a computer monitor represent the impacted database and indicate that it is currently in danger.

The existence of an attacker or cybercriminal who caused the breach is symbolized by the hacker icon, which is a hooded figure holding a laptop.

Open book and folder: Showcase common library materials that may be impacted, whether they are digital or physical (e.g., user records, borrowing history, research data).

This picture essentially alerts library employees or patrons to a significant cybersecurity event that may require quick action to safeguard data or look into the breach.

OVERVIEW OF EXISTING NIGERIAN LIS CURRICULA

Nigerian LIS Curriculum Trends

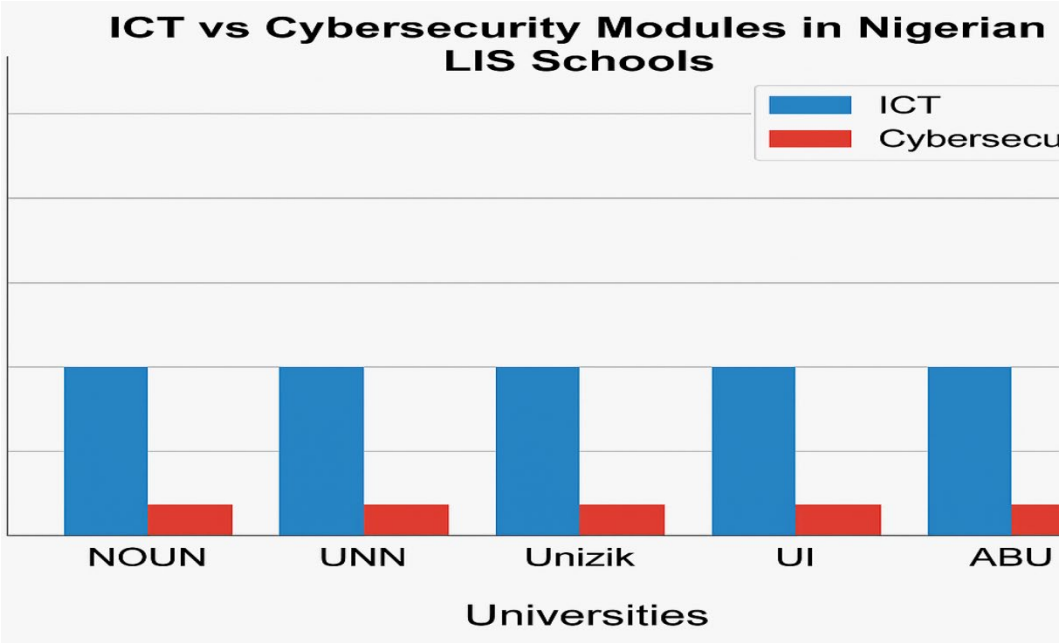
Nigerian LIS programs increasingly incorporate digital librarianship, according to recent studies and handbooks, but they mostly lack explicit training on artificial intelligence (AI) or cybersecurity (Kwanya et al., 2024; Elebiju, 2024). For instance, the majority of recognized LIS programs in Nigeria currently provide a stand-alone course on "Digital Libraries" or a comparable topic (such as NOUN's LIS 407: Management of Digital/Virtual Libraries).UI's LIS 114: Introduction to Digital Libraries (ui.edu.ng) and nou.edu.ng. According to Okeji and Mayowa Adebara (2021), the majority of library schools in Nigeria incorporate lessons on digital libraries into their core curriculum. Instead of being taught as stand-alone modules, metadata skills are primarily taught in cataloguing/classification or "information organization" courses. For example, there are several cataloguing and classifying courses listed by NOUN and Unizik, which suggests metadata training, but there isn't a single "metadata" course.

Gaps: There are typically no specialized cybersecurity or artificial intelligence courses in Nigerian curricula. Many LIS schools in Nigeria continue to use antiquated curricula and have "not adequately incorporated emerging technologies such as artificial intelligence, digital libraries, and cloud computing," according to a recent evaluation (Jegbefume et al., 2025). Even though libraries are becoming more and more dependent on digital technology, cybersecurity is rarely covered in professional training or the curriculum. Limited ICT infrastructure also makes practical training difficult. For instance, only a small percentage of LIS departments in Nigeria have computer labs that are adequately prepared to teach digital library skills (researchgate.net). This is consistent with research showing that staffing and infrastructural limitations hinder the incorporation of contemporary technology into Nigerian LIS education (researchgate.netjeweljournals.com).

Emerging Best Practices: Programs are being revised to better meet the demands of the present. According to the literature, cybersecurity and AI courses should be added. In order to address changing user needs, Jegbefume et al. (2025) especially call for Nigerian LIS curriculum to "develop competencies in artificial intelligence applications [and] cybersecurity."jeweljournals.com. In LIS trainingresearchgate.net, international standards (such

IFLA) also place a strong emphasis on metadata, networks, and digital archives. Inter-disciplinary approaches are suggested by best practice examples, such as incorporating ICT modules into librarianship courses and working with computer science (as demonstrated in programs that co-teach IT skills). While there are still gaps in formal cybersecurity and artificial intelligence issues, some Nigerian colleges are reacting by providing courses like "Information Systems Analysis" or "Automation in Libraries" (e.g., Unizik LIS 405 on library automationeducation.unizik.edu.ng).

Bar chart showing absence/presence of ICT vs cybersecurity modules



The bar chart (Fig. 5) shows all five Nigerian LIS schools include ICT modules, but none offer dedicated cybersecurity training, highlighting a significant curriculum gap.

Table 2: Comparing course content across 4–5 Nigerian LIS schools

Course Module	University of Ibadan	Ahmade Bello University	University of Nigeria, Nsuka	Bayero University	University of Ilorin
Cataloguing and Classification	✓	✓	✓	✓	✓
ICT in Libraries	✓	✓	✓	✓	✓
Records Management	✓	✓	✓	✓	✓
Information Retrieval Systems	✓	✓	✓		✓
Cybersecurity Awareness					
Digital Preservation	✓		✓		✓

Table 2 identifies curriculum modernization gaps by highlighting which institutions have implemented contemporary modules such as Cybersecurity Awareness and Digital Preservation. The analysis that follows focuses on how current capabilities like cybersecurity, digital librarianship, metadata, and artificial intelligence (AI) are included into undergraduate LIS courses at Nigerian universities. Additionally, I will contrast these results with comparable undergraduate LIS programs at foreign universities. In addition to highlighting trends and providing opinion on gaps and best practices, I will present a comprehensive table that summarizes course coverage across the institutions.

Integration of Modern Competencies in LIS Curricula

The author of this paper examined current undergraduate Library and Information Science (LIS) programs in Nigeria as well as a few institutions abroad. Using source-based evidence of pertinent courses, Table 1 analyzes whether each program specifically addresses cybersecurity, digital librarianship, metadata, and artificial intelligence in libraries.

Table 3: Comparism of Universities and program explicitly covers cybersecurity, digital librarianship, metadata, and AI in libraries

Institution (Program)	Cybersecurity	Digital Librarianship	Metadata	AI in Libraries
Nigeria: National Open Univ. (NOUN)	No dedicated course	**Yes:** e.g. *LIS 407 Management of Digital/Virtual Libraries*, *LIS 416 Introduction to Digital Information Systems & Services*	*Implied:* core cataloguing/classification courses exist (e.g. *Information Retrieval/Cataloguing*), but no standalone metadata course	No
Nigeria: Univ. of Nigeria, Nsukka (UNN)	No (no course on security found)	**Yes:** *LIS 402 Contemporary Technology in Libraries* covers ICT/digital tools	Yes (intro to cataloguing/classification is taught)	No
Nigeria: Nnamdi Azikiwe Univ. (Unizik)	No	**Yes:** *LIS 311 Internet and Electronic Libraries* explicitly teaches digital library concepts	Yes (courses in Indexing/Abstracting and Classification)	No
Nigeria: Univ. of Ibadan	No	**Yes:** *LIS 114 Introduction to Digital Libraries*	Yes (Information organization taught in core courses)	No
USA: Catholic Univ. of America (MS in LIS)	No	**Yes:** offers *LSC 612 Foundations of Digital Libraries*	**Yes:** includes *LSC 615 Metadata*	No
USA: Univ. of Washington (MSIM)	**Yes:** specialization includes *IMT 555 Foundations of Cybersecurity*	Partial (digital topics in electives)	Core info organization courses cover metadata implicitly	No (not a focus)
UK: Robert Gordon Univ. (CPD)	– (addresses security/privacy issues)	**Yes:** Digital Libraries short course (privacy & security topics)	–	–

Institution (Program)	Cybersecurity	Digital Librarianship	Metadata	AI in Libraries
South Africa: Univ. of Pretoria (BS Information Science)	Emphasizes cybersecurity/AI in ICT modules (dept. focus)	Yes (modules on Digital Repositories) research	Yes (information organization courses)	Emerging (AI discussed in research context)

The coverage of contemporary competencies in a few chosen LIS programs is displayed in Table 3. (Yes/No denotes specific courses; when appropriate, partial coverage is indicated. Official program descriptions or curriculum are cited in the references).

INTERNATIONAL PROGRAM HIGHLIGHTS

More often than not, international LIS/information programs include these competencies:

Digital Librarianship and Metadata: Specialized courses are offered in many US and UK programs. For instance, the LIS track at Catholic University of America offers a course on digital libraries (LSC 612) as well as a course specifically on metadata (LSC 615) (Catholic University of America, 2025). Information architecture, metadata management, and digital curation are all covered in the same way by iSchools in the UK and Canada. These programs have a strong emphasis on organizing information and managing digital collections from start to finish. A wide focus on digital librarianship is shown in the Robert Gordon University (UK) digital libraries program, which specifically addresses user needs and system security concerns (privacy, data protection, etc.) (Robert Gordon University, 2025).

Cybersecurity: Content about cybersecurity is now included in certain international information programs. "IMT 555: Foundations of Cybersecurity," which covers security principles for information professionals, is part of the MS program in Information & Cybersecurity offered by the University of Washington's Information School.To train information management professionals to lead cybersecurity technical projects and information security teams, iSchool.uw.edu and IMT 559 Cybersecurity Functions and Trends explore cybersecurity technologies from a technical leadership viewpoint (University of Washington, 2025). This demonstrates how LIS/Info curricula are increasingly incorporating cybersecurity concepts (networks, incident response, and risk frameworks). Security is similarly addressed in South African and Canadian degrees (typically under "Information Science"); for instance, the University of Pretoria emphasizes cybersecurity and artificial intelligence (MIT 889) in its information science research and curriculum.up.ac.za.

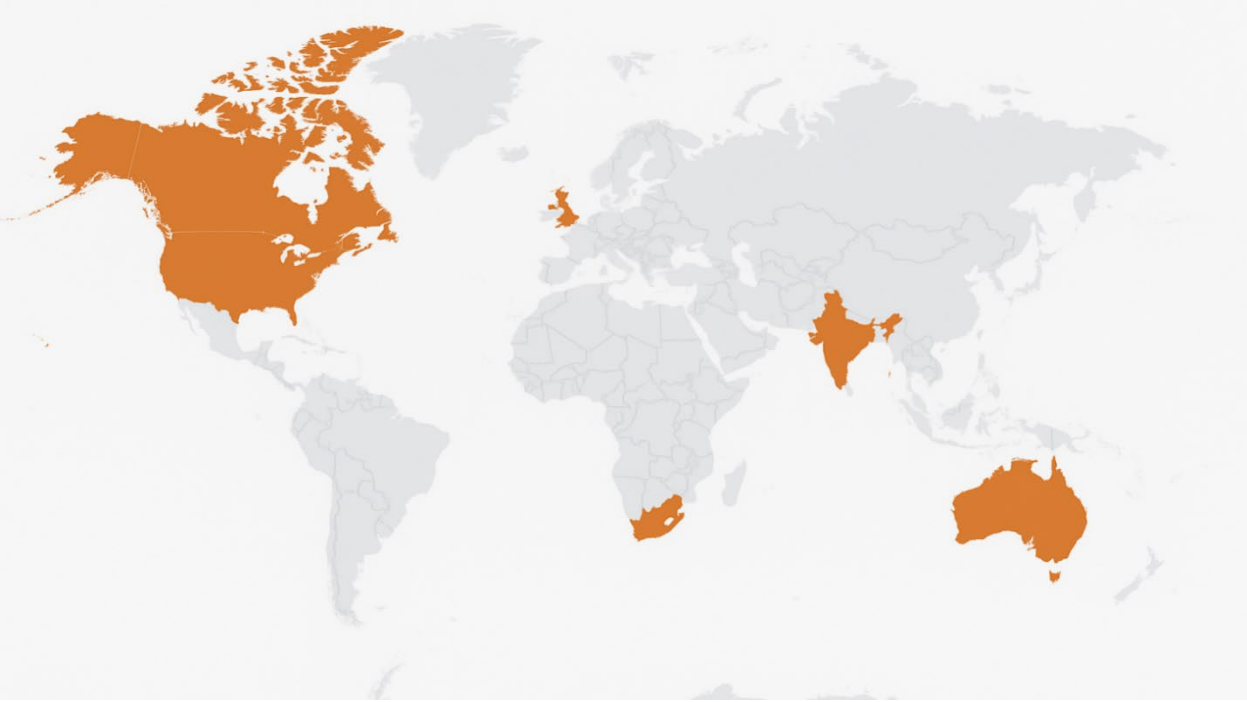
Artificial Intelligence: Even abroad, formal AI courses in LIS degrees are still uncommon. But there is an increasing emphasis on professionalism. AI's importance is highlighted by recent publications and open educational materials, such as Reddy (2024), which address subjects including machine learning, natural language processing, and ethical library use. Although it is not yet widely included in undergraduate LIS curriculum, AI is being introduced more and more in

master's programs and continuing education courses on subjects including digital content production, data analytics, and discovery systems. In order to establish familiarity, best practices include starting with modules on "AI in libraries" or incorporating AI technologies into information retrieval courses.

Observably, Nigerian LIS courses now adequately reflect digital librarianship (online services, digital libraries), in accordance with global emphasis (researchgate.netlis.catholic.edu). All programs cover metadata (typically through cataloging classes). However, advanced LIS programs overseas are beginning to incorporate cybersecurity and artificial intelligence (AI) (e.g., through specialist tracks or elective courses) but Nigerian undergraduate LIS programs largely lack these topics (Onyema et al., 2021; Osijinrin et al., 2025). Nigerian LIS education would be in line with new international standards and professional demands if these gaps were filled by including courses on information security, machine learning applications, and real-world digital projects.

INTERNATIONAL BENCHMARKS AND BEST PRACTICES

World Map Snapshot



With new initiatives in Nigeria and other African countries, Fig. 6 shows which countries are most notable for integrating cybersecurity into LIS or similar information-security programs: the USA, UK, South Africa, India, and Canada.

Table 3: Nigeria vs. Other Nations: Side-by-Side Curriculum Comparison

Element	Nigeria	USA	UK	South Africa	India
Program level	New NUC Core Course (2023) across all degrees including LIS (Ayo-Odewale, 2023)	Diverse: e.g., UW iSchool BS concentration; UC Berkeley MICS; UIUC electives	Integrated into MA/MSc at UCL, Royal Holloway MSc Info Security	MSc InfoSec @ Pretoria; diplomas @ UCT, CPUT, UJ	MSc Cybersecurity & Digital Forensics @ KL University
Curriculum format	Mostly embedded modules plus optional full programs; vocational CCNA etc.	Both stand-alone and embedded; strong privacy & ethics emphasis	Both dedicated and embedded; includes digital forensics in LIS courses	Strong full MSc with labs, diplomas focusing hands-on skills	Specialized MSc; focuses on network defence, forensics, incident response
Core topics	NDPA 2023, Cybercrimes, basics of sec. + CCNA-cert prep, labs	Info assurance, privacy law, cryptography, secure programming	Governance, digital forensics, ethics, cryptography	Network security, risk mgmt, encryption, forensics, practical labs	Network defense, data forensics, incident response, labs
Practical components	Hands-on labs, CCNA tracks, internships via 3MTT	Lab-based courses; capstone projects; ethical hacking drills	Forensic simulations; policy drafting; case studies	Full practical modules, industry partnerships	Lab exercises; forensic casework; incident response labs
Ethics & legal framework	Emerging – NDPA adoption, Cyber ethics awareness	Strong focus on privacy, ethical hashing, policy compliance	Ethics, intellectual freedom, GDPR alignment	Policy-driven with national compliance focus	Privacy law, ethical hacking on curricula

Table 4: Examples from LIS curricula in the US, UK, South Africa, India, etc.

Country	Institution / Program	Integration Approach	Core Cyber Topics
USA	University of Washington iSchool (BS Informatics)	Dedicated cybersecurity & privacy concentration	Info assurance, privacy law, network and system security (University of Washington Information School, 2025)
USA	UC Berkeley School of Information (MICS)	Stand-alone expert master's in cybersecurity	Cryptography, OS security, privacy engineering, legal/ethical aspects
USA	UIUC (University of Illinois at Urbana-Champaign) Cyber-Security Ethics (graduate elective)	Case-study ethics-based course	Immersive ethical dilemmata, debate-based learning
UK	Royal Holloway, University of London (ISG MSc in Info Security)	Specialized MSc in Information Security	Governance, cryptography, forensics, network security
UK	UCL Department of Information Studies (MA/MSc LIS accredited by CILIP & ALA)	Integrated cybersecurity modules	Ethics, privacy, digital forensics (embedded in wider LIS degree)
UK	Sheffield iSchool	Embedded security in undergraduate & postgraduate	Policy, HCI security, info retrieval safety
South Africa	University of Pretoria (MSc Info Security)	Full MSc in Information Security	Network security, risk management, data protection (includes labs & research)
South Africa	UCT Postgrad Diploma, CPUT Diploma, UJ BSc Cybersecurity	Vocational qualifications with practical focus	Digital forensics, penetration testing, legal issues
India	KL University MSc Cyber Security & Digital Forensics	Specialized master's in tech domain	Network defense, data forensics, incident response

Case Studies: Successful Curriculum Integration

1. Illinois University in Urbana Champaign. A course on Graduate-level Cybersecurity Ethics (USENIX ASE 2018) at the University of Illinois, according to Blanken-Webb et al. (2018), demonstrated enhanced awareness of "ethical unknown unknowns" and

embedded ethical decision-making within real-case scenarios. Information exchanges, debates, and a community of practice foster moral reasoning.

2. In a case study on cybersecurity education in higher education conducted throughout the United Kingdom (IEEE FIE, 2019), Tom Crick et al. From comprehending the relationship between hardware and software, moving from theory to practice (and vice versa), to human factors, policy, and politics (as well as numerous other significant aspects), the perspective offers a national case study-based analysis of the many facets of cybersecurity education and how they are prioritized, implemented, and accredited. In recent years, numerous model curricula and proposals have been considered and presented in international forums, with differing degrees of influence on practice, policy, and education. The study answered three important questions: i) what is taught and what should be taught to general computer science students about cybersecurity; ii) should cybersecurity be taught to general computer science students in an integrated or stand-alone manner; and iii) can accreditation by national professional, statutory, and regulatory bodies improve cybersecurity provision within a body's jurisdiction? The author assesses cybersecurity education across the board as a problem of evidently significant magnitude. Rather, a case study-based research methodology was used to assess the evidence of teaching cybersecurity to university-level students as part of mainstream computer science, with a primary focus on the UK. What does the need to incorporate cybersecurity knowledge and skills mean more broadly for institutions and educators, and how can we better teach this subject in the context of the global reform of computer science and engineering curricula? This UK case study illustrated the beneficial impact of national accreditation requirements and provided some suggestions for future research and curriculum development by comparing it to similar programs in the US. Broader competency is fostered by the cybersecurity course integrated into foundational computer science or information courses. Curriculum uptake can be greatly influenced by accreditation organizations (such as CILIP, ALA, and QAA), and sustainability depends on integrating theory with real-world labs and human factors.
3. In accordance with the most recent cybersecurity curriculum standards, such as CSEC2017, the Royal Holloway ISG (RULIS) Program: MSc Information Security (since 1992) has promoted the integration of cybersecurity as a cross-cutting concept in CS curricula. We report on our experience teaching over 2200 students in three undergraduate core computer science courses at a top technical institution in Europe between 2018 and 2023 by applying this cross-cutting intervention. A security expert and the appropriate course instructor collaborated to integrate security education into computer science courses. The security expert created and presented lectures that covered a variety of CSEC2017 topic areas after consulting with the course instructors. This resulted in a complicated relationship between the students, the security specialist, and the course instructor. We examine our intervention from the viewpoints of the three stakeholders: we gathered student opinions through a post-course survey and assessed their experiences through semi-supervised interviews with the security expert and responsible course instructors. The misaligned incentives for the teachers and the security expert made it impossible to sustain this intervention without organizational support,

even though the students were very excited about the security material and continued to feel its effects years later. The intervention's limits are identified, and suggestions for maintaining it are provided. Highlights include the world's oldest university-based master's degree in cybersecurity; a blend of demanding technical courses with forensic practice, real-world case studies, and policy; and acknowledgment through national achievement awards (ACE-CSR status, Queen's Anniversary Prize).

CASE HIGHLIGHTS AND PERSPECTIVES

Nigeria: National University Commission CCMAS Update (2023) released by Ayo-Odewale (2023) said that cybersecurity is now a core course across Nigerian universities, including in LIS and associated degrees (Ayo-Odewale, 2023). The research highlighted Early Education Push initiatives, such as BusinessDay and Edugist, which promote cybersecurity education starting in secondary school and incorporate CCNA certificates and practical lab courses (Oladuso, 2024). Additionally, the Capacity-Building 3MTT: National program opened doors for LIS professionals by teaching 3 million Nigerians digital skills, including cybersecurity.

LIS undergraduates can specialize in information security and privacy at the University of Washington iSchool, which covers assurance, legal requirements, and system integration. The UC Berkeley MICS Program is a thorough master's program that includes privacy engineering, OS security, and cryptography. The UIUC Cyber Security Ethics Elective, which involves students in in-depth case studies and discussions on cybersecurity ethics, should also be included.

UK: One of the first in the world, the Royal Holloway MSc in Information Security is a well-known comprehensive program that combines labs, policy, and forensic practice. Modules on ethics, privacy, and digital forensics are integrated into the core information studies curriculum of the UCL LIS MSc/MA.

South Africa: Participating was the University of Pretoria MSc InfoSec structured program with an emphasis on research and lab; UCT, CPUT, and UJ diplomas prioritize vocational training that prepares students for the workforce.
India: Supported by lab work, the MSc Cyber Security and Digital Forensics program at KL University is a highly specialized curriculum that covers network defense, forensics, and incident response.

BEST PRACTICES AND RECOMMENDATIONS

The case studies offer some advice and best practices that are thought to be highly significant. They consist of, but are not restricted to:

Embedded vs. Dedicated Modules: Both embedded security modules (UCL, Sheffield) and stand-alone programs (e.g., MICS at Berkeley, MSc at Royal Holloway) work well. While specialized tracks develop highly specialized abilities, embedded techniques assist all LIS students in gaining a basic understanding of security.

Blended Pedagogy: To cover the entire range of cybersecurity, effective courses combine technical laboratories (such as penetration testing and encryption) with policy, ethics, and case-based learning.

Adoption Driven by Accreditation: The UK model demonstrates how consistent integration across programs is fueled by institutional accreditation (e.g., CILIP, ALA, QAA, IEEE FIE frameworks).

Emphasis on Ethics and Human Factors: Courses such as UIUC's case-based ethics emphasize how crucial it is to train librarians in both the technical aspects of data stewardship and the moral issues involved.

Project and Simulation-Based Learning: Immersion learning methods, such as group incident-response drills and real-world breach simulations, increase confidence and participation.

RESULTS OF A NARRATIVE LITERATURE REVIEW ON NEW TOPICS IN CYBERSECURITY AND LIS

A review of the literature and research on new topics in cybersecurity and LIS are available. A notable aspect in the list is the following.

Awareness and Capacity Building: A study by Oladokun et al. (2024) from Southeastern Nigeria demonstrate low overall cybersecurity competency among librarians with deficiencies in cyber incident detection and prevention and advocate for continued training and infrastructure investment. The study indicated that university libraries may face dangers, such as line tapping, faulty system processing, and the use of harmful software. These risks have serious repercussions, including the possible loss of private information, harm to one's reputation, and monetary losses. Thus, the study looked at cybersecurity threats in African university libraries and the necessity of encouraging cyberethical behavior. The highlighted the complexity of cybersecurity threats, including ransomware, phishing, malware assaults, and identity theft. If left unchecked, these dangers can have serious repercussions, such as financial losses, reputational harm, and theft of intellectual property.

Organizational Justice and Behavior: Research in South East Nigeria shows that equitable organizational climates enhance librarians' compliance with digital security procedures such as password hygiene, backups, and antivirus software; yet, awareness training is still infrequent (Okpara et al., 2024).

Crisis and Security Management: According to Nigerian assessments, university libraries are susceptible to calamities and hacking due to a lack of disaster response teams and inadequate preparedness frameworks (Fatade et al., 2023).

Ethics and Cyberethics Promotion: Infrastructure limitations and resource shortages impede the promotion of responsible online activity, and Nigerian postgraduate librarians frequently lack knowledge of cyberethical norms (Dunmade & Tella, 2023).

Holistic Cyber-resilience: Digital library experts interviewed highlight a three-pillar strategy that anchors cybersecurity in risk assessment and ongoing improvement: governance, awareness, and technology (Bellini & Tammaro, 2023).

These topics, which are depicted in the concept map above, indicate a literature emphasis on awareness, behavior, policy/guidance, and resilience/capacity.

THEORETICAL FOUNDATIONS

Information Security Theory: The CIA triad—Confidentiality, Integrity, Availability is cited in works as being fundamental to organizational justice, governance, and library security planning. It also provides theoretical backing for stakeholder and policy participation (Osaro & Osazuwa, 2024). A fundamental framework for comprehending how to defend information assets against threats and vulnerabilities is provided by information security theory (Taherdoost, 2022). It highlights the CIA Triad—Confidentiality, Integrity, and Availability—as fundamental concepts in cybersecurity. Only authorized users may access information thanks to confidentiality, data is shielded from unwanted changes by integrity, and systems are available when needed thanks to availability. The idea directs the application of risk assessments, technical controls, and regulations to stop insider threats, cyberattacks, and data breaches. In the context of cybersecurity, it enables organizations to create structured, proactive strategies to secure digital environments against evolving threats and human or technical vulnerabilities. Information security theory is used in Nigerian libraries and universities to protect user data, digital resources, and academic records. Network access controls, data encryption, and user authentication are all guided by the CIA Triad. To maintain system availability and safeguard privacy, libraries use firewalls, antivirus programs, and password rules. Universities often do data backups and audits to preserve data integrity and lessen cyberthreats. Full adoption is hampered by issues including obsolete infrastructure, low cybersecurity knowledge, and insufficient financing. In spite of this, the idea guides expanding efforts to create institutional cybersecurity policies and increase capability through strategic IT planning and training.

Digital literacy and cyberethics: Based on well-known digital literacy models (such as IFLA and ALA), they include cyberethics instruction that addresses safe online behavior, plagiarism avoidance, and attribution all of which are currently lacking in many Nigerian LIS programs (Dunamde & Tella, 2024). Effective use of digital tools and an ethical awareness of online behavior are combined in the Digital Literacy and Cyberethics Framework. In addition to raising awareness of privacy, intellectual property, cyberbullying, and online security, it places a strong emphasis on developing the ability to navigate, assess, and produce digital information responsibly. It helps faculty and staff in academic institutions interact critically and morally with digital environments. By promoting courteous communication and well-informed decision-making, the framework promotes responsible digital citizenship. It is essential for preparing individuals to thrive in the digital age while upholding ethical standards, protecting personal data, and contributing positively to digital communities.

Socio-technical and Risk Management Frameworks: New research supports a multifaceted strategy that links technology, staffing, and processes, as demonstrated by NIST and NIST adaptations in digital libraries (Bilini, 2024). Frameworks for risk management and sociotechnical

analysis acknowledge that cybersecurity is a multifaceted problem with organizational, technological, and human components. In order to guarantee secure information systems, the socio-technical framework places a strong emphasis on coordinating people, procedures, and technologies. When managing digital environments, it takes institutional culture, policy adherence, and user behavior into account. In the meanwhile, the risk management framework uses systematic techniques including risk analysis, control implementation, and monitoring to identify, evaluate, and reduce any threats to information assets. In settings like Nigerian academic institutions, these frameworks operate together to create a comprehensive cybersecurity strategy that strikes a balance between technology controls, human awareness, governance, and strategic decision-making.

To improve cybersecurity, the risk management and socio-technical frameworks can be used. By implementing digital literacy training, enhancing ICT infrastructure with multi-factor authentication, and revising policies, the socio-technical strategy brought people, technology, and processes into alignment. To supervise implementation, a cross-functional cybersecurity committee was formed. As part of the risk management framework, controls like email filters and access protocols were put in place, threats including insider misuse and phishing were identified, and their effects were evaluated. Mechanisms for user reporting and routine audits were implemented for monitoring. These frameworks increased trust in UNILAG's online learning environment, decreased incidents, and raised security awareness.

LIS PROFESSIONALS' PREPAREDNESS: EVIDENCE FROM THE LITERATURE

Low Technological Competence: In order to store information in university libraries in southeast Nigeria, Obim and Akpokurerie (2023) concentrated on librarians' awareness of cybersecurity. The authors aimed to identify the different cybersecurity threats in Southeastern Nigerian university libraries, evaluate the cybersecurity competency of librarians for effective information storage in Southeastern Nigerian university libraries, determine the degree to which the cybersecurity competency of librarians contributes to effective information storage in Southeastern Nigerian university libraries, identify the obstacles to acquiring pertinent cybersecurity awareness among librarians for effective information storage in Southeastern Nigerian university libraries, and offer solutions to improve the acquisition of pertinent cybersecurity awareness among librarians for effective information storage in Southeastern Nigerian university libraries. The results showed that, among other things, hacking, impersonation, electronic message interception, unlawful access to information resources, and computer viruses were the main cybersecurity concerns in university libraries. Due to a number of factors, including poor technology infrastructures, a lack of a cybersecurity policy framework in university libraries, and insufficient training on cybersecurity measures, librarians have a low level of cybersecurity competency for efficient information storage. Among other things, the report suggested that librarians receive ongoing training on cybersecurity measures, particularly in the areas of detection and prevention. administration of the university library. Because of inadequate training, shoddy infrastructure, and a lack of policy frameworks, librarians in Southeastern Nigeria score badly on cybersecurity competency tests.

Positive Impact of Institutional Fairness: Okpara et al.'s (2024) study, which examined Organizational Justice and Librarians' Digital Security Practices in South-East Nigerian Universities, found that, among security behavior indicators, protecting mobile devices, using antivirus software, scheduling backups, and installing firewalls were the most frequently used digital security practices by librarians in South-East Nigerian university libraries. The results also showed that although the respondents do not take part in yearly security awareness training, they occasionally tried creating strong passwords and safeguarding devices. The results additionally demonstrated that all three aspects of organizational justice procedural, distributive, and interactional justice showed high levels. The study also demonstrates that librarians' security behavior in South-East Nigerian university libraries is positively and significantly impacted by organizational justice. Higher use of security practices, such as firewalls, backups, and antivirus software, is correlated with strong distributive, procedural, and interactional fairness; however, training uptake is low.

Cyberattack and Disaster Vulnerability: Fatade et al. (2024) examined security management and disaster preparedness in two university libraries in South-West Nigeria. According to the study, hacking poses a serious security risk to university libraries, especially those that have e-libraries. Research indicates that academic institutions and e-libraries in southwest Nigeria are vulnerable to issues including hacking and a lack of preparedness for disasters. Among other things, the authors suggested that academic libraries establish disaster response teams to handle emergencies.

Absence of Cyberethical Engagement: Dunmade and Tella (2023) investigated how libraries and librarians might encourage postgraduate students in Nigeria to behave appropriately online. The study found that two major obstacles to advancing cyberethics are postgraduate students' ignorance of cybersecurity threats and the need for librarian training and resources. According to reports, Nigerian academic librarians lack the necessary policy framework and training to effectively model and encourage cyberethical behavior. The author invited librarians to take the lead in cyber resilience and advocated for the integration of cybersecurity through governance, awareness, and technological solutions. Cybersecurity in university libraries and its implications for teaching library and information science (Igbinovia and Ishola, 2023). According to the study, librarians' perceived level of cyber security awareness was mediocre. The university libraries were also subject to a number of cyberthreats, and one of the most important ways to prevent cybercrime is to implement cyber security and guidelines. Additionally, the results demonstrated that librarians adhered to cyber ethics to a great degree. However, the primary obstacle to the implementation of cyber security in university libraries was found to be the attitude of library administration toward cyber security concerns, which was followed by inadequate password management. Although they are very interested in learning more, the majority of librarians only have rudimentary knowledge of cyber security. They expressed a desire to learn more about cyber security, even if it was not covered in library school. Due to a shortage of qualified personnel, the majority of library schools do not provide cybersecurity courses, according to the results of the interview with their leaders.

The aforementioned makes it evident that there is awareness and competence. Because of inadequate infrastructure, policy, and training, gaps still exist among Nigerian LIS experts. The fact that justice and organizational environment improve adherence to security procedures and that

policy inclusion promotes resilience is also noteworthy. Additionally, cyberethics is still in its infancy; librarians can play a bigger part in setting an example of appropriate online behavior. The results also show that holistic approaches that integrate technology, awareness, and governance in line with frameworks such as NIST are regarded as best practices. Finally, Nigerian libraries lag but have clear improvement pathways; resilience necessitates integration across training, infrastructure, regulations, and ethical advice. Based on these results, the Nigerian LIS curriculum can be improved by integrating policy analysis, ethical discussions, and practical laboratories into a robust socio-technical framework.

IMPLICATIONS OF CURRICULUM MODIFICATION

The curriculum modification discussed in this paper has implication for academic, professional and institutional. These are discussed in turn as follows:

Academic Implications

Adding cybersecurity to Nigeria's LIS curriculum would greatly increase students' skill sets. Graduates would require a foundation in data privacy and governance (knowing Nigeria's 2023 Data Protection Act, or NDPA, and its regulations), as well as information security (e.g., threat types like malware, phishing, and ransomware, and protective measures like encryption and access control), according to Nakiyingi (2024). In addition to traditional library abilities, they would acquire multidisciplinary skills based on computer science, law, and management, such as the fundamentals of network and system security, safe data storage, and digital forensics. In actuality, this entails including classes or modules on risk assessment, digital asset security, safe metadata/cataloguing, and cyber-ethical behaviors.

Since the current NUC mandate requires LIS programs to provide students "with relevant theoretical knowledge, practical skills and techniques" (NUC, 20014; NUC, 2014), cybersecurity topics would expand these goals into the digital sphere. The NUC standards for LIS already place a strong emphasis on broad ICT knowledge. According to experts, Nigerian LIS curricula now notably lack contemporary IT innovations including cybersecurity, cloud computing, artificial intelligence, and the Internet of Things (Dahiru, 2022). Professional organizations like IFLA are now calling for libraries and their employees to receive cybersecurity and digital literacy training and resources in accordance with international standards (IFLA, 2022). Similarly, IFLA has previously acknowledged the importance of teaching digital preservation and curation, which equips students to maintain and protect digital collections, protecting cultural heritage and creating new professional opportunities (Oyelude, 2023). Summarily, incorporating cybersecurity would enhance LIS competences (information ethics, law, and organization) and meet both national Core Curriculum Minimum Academic Standards (CCMAS) requirements and international best practices by adding competencies in secure information handling, digital infrastructure management, and privacy law.

The following are only a few of the anticipated new main competencies:
Understanding cyberthreats, encryption, authentication, and access restrictions (patron privacy, system integrity) are all components of secure information management (Nakiyingi, 2024).

Understanding NDPA regulations, GDPR counterparts, and user data rights is essential for enabling positions such as Data Privacy Officer and maintaining data privacy and legal compliance. For instance, the NDPA mandates that large corporations appoint a Data Protection Officer who is knowledgeable on privacy law (Alliance Law Firm, 2024). These regulations and their implications for libraries and archives would be studied by LIS students.

In accordance with IFLA's guidelines for libraries to "promote online safety," cyber-ethical and digital literacy skills include educating users' safe practices and how to critically evaluate digital content (IFLA, 2022).

Digital preservation and curation: applying library science to metadata curation, digital repositories, and digital archives (IFLA, 2022). This includes using techniques that maintain authenticity over time and maintaining born-digital content (such as institutional repositories and digitized archives).

Interdisciplinary integration: connecting management (information governance, auditing processes) and computers (network fundamentals, database security). By including specialized IT security modules, the curriculum may expand on already-existing courses such as "Information Ethics and Law" (LIS 411 Information Ethics and Law (NUC, 2015) is already included in NUC MAS).

These enlarged competencies are in accordance with international frameworks (IFLA's Cybersecurity Statement and digital curation recommendations) and Nigerian educational requirements (NUC MAS supports ICT competency in LIS, 2015), which place an emphasis on both technical skills and user-centric information ethics.

For the suggested module and contents to included at both undergraduate and graduate level on Cybersecurity in Library and Information Science, please, see Appendix 1.

Professional Implications

A cybersecurity-enhanced LIS program would prepare graduates for a range of emerging information roles. These include the following:

Digital Curator/Archivist: By managing institutional digital archives, librarians with cybersecurity expertise can guarantee the preservation and long-term accessibility of digital heritage. According to recent research conducted in Nigeria, training in digital curation opens up new job options in museums, libraries, and archives (IFLA, 2022). Graduates would be skilled in implementing preservation standards, managing metadata, and creating safe digital archives.

Data Privacy Officer: Numerous public and private organizations are required to designate Data Protection Officers in accordance with Nigeria's NDPA. Graduates with a background in LIS who have also received privacy and security training are well-suited for this position. In fact, companies are required by Section 32 of the NDPA to appoint a Data Protection Officer who is knowledgeable about data protection laws and procedures (Alliance Law Firm, 2024). LIS

graduates who are already proficient in records administration and information ethics could work as DPOs, managing privacy policies and compliance audits.

Information Governance Analyst/Records Manager: Businesses are in greater demand of experts to create and implement data governance and compliance rules. Graduates of advanced LIS programs would be eligible for analyst positions in the public sector, private sector, or healthcare industry, where they would be able to align information systems with legal requirements (such as the NDPA and FOI legislation). (This overlap is reflected in the fact that many job advertisements for "Information Governance Analysts" specifically state that library/information science degrees are accepted.) These positions make use of librarians' knowledge of information organization, which is now strengthened by their proficiency in cybersecurity risk assessment.

Cybersecurity Liaison/Instructional Specialist: Librarians can act as a liaison between IT security teams and library employees or patrons in academic or public library contexts. Trained as cybersecurity liaisons, they would work together on incident response, offer advice on how to use library networks securely, and instruct users on safe computer practices. (For instance, to represent this new specialty, librarians at certain institutions now have titles like "Systems Librarian" or "Cybersecurity Liaison.")

These positions have definite advantages for employability. Such hybrid skill sets are in high demand, according to the labor market. For instance, a cybersecurity training track is specifically included in the Federal Ministry's 3MTT (3 million Tech Talents) project (Oloruntade, 2024). highlighting the demand for cybersecurity experts in Nigeria. Graduates become competitive candidates for the same growing industries that the 3MTT program is targeting by incorporating related topics into LIS education. Librarianship graduates will not fall behind in the digital economy if the LIS curriculum is in line with national tech strategies (such as NDPA and 3MTT).

Institutional Implications

At the departmental and university level, adding cybersecurity to LIS education will require substantial capacity building. Major considerations include:

Faculty Expertise: There aren't many cybersecurity-focused faculty members at Nigeria's current LIS institutions. "The majority [of LIS schools] do not offer [cybersecurity] courses due to a lack of skilled manpower," according to a recent study (Igbinovia & Ishola, 2023). Institutions would have to hire qualified teachers (such as those with credentials in computer science or MLIS+IT) or help current lecturers advance their careers. This could entail collaborative appointments between the ICT and LIS departments or professional development initiatives (certifications, workshops) to teach librarians about cyber issues.

Curriculum Development: Departments are required to either create new courses or update current ones. LIS schools are able to provide elective cybersecurity modules because of NUC's 70:30 structure, which consists of 70% core CCMAS and 30% university-developed content (TechTrends, 2024). To incorporate industry-relevant material (network security, the fundamentals of ethical hacking, etc.) into the curriculum, they ought to establish curriculum

committees with cyber specialists on them. It might also be necessary to coordinate with regulatory organizations (such as the Librarians' Council of Nigeria and NUC) in order to validate the amended program.

Technical Resources: Interactive facilities are necessary for effective cybersecurity instruction. Computer labs with secure servers for practice, simulation software (for firewalls, intrusion detection, etc.), and network monitoring tools would be beneficial to LIS departments. It is crucial to invest in modern ICT infrastructure, such as dependable internet, virtualization labs, and cyber range platforms. Additionally, libraries may subscribe to pertinent databases or security training platforms and grow their digital collections (for teaching digital curation).

Training and Partnerships: Universities can collaborate with the government (such as the Nigeria Data Protection Commission or NITDA), non-governmental organizations, or business to offer internships, training workshops, and guest lectures in order to close the first gaps. For instance, governments are urged to "ensure libraries have the resources and training" to develop cybersecurity capabilities, according to the IFLA Cybersecurity Statement (IFLA, 2022). In actuality, this can entail using grants or national programs (such as 3MTT clusters) to train LIS instructors and students. Working together with cybersecurity and IT companies in Nigeria may also yield real-world case studies and mentorship.

Last but not least, current academic members and librarians will require continual upskilling. Institutions may incorporate cybersecurity instruction into their professional development programs (e.g., by offering certification courses to current librarians). Long-term support for the new curriculum will come from creating a culture of ongoing learning (via research, conferences, and interdisciplinary seminars).

In conclusion, significant adjustments to material and human resources will be necessary to update the LIS curriculum. It will be essential to hire or train experienced instructors, set aside funds for labs, and establish connections with the sector. These investments would put Nigerian LIS departments in a position to support the nation's larger digital education strategy (such as NDPA compliance and 3MTT goals) and align with NUC's technical requirements, which now include cybersecurity among core courses (TechTrends, 2024).

CHALLENGES AND CONSIDERATIONS

The growing integration of digital technologies in libraries and information systems has made cybersecurity a vital competency for Library and Information Science professionals. However, incorporating cybersecurity education into the LIS curriculum presents several interrelated challenges and considerations. These include but are not limited to:

Limited Faculty Cybersecurity Expertise: One of the biggest problems is the lack of LIS professors with official cybersecurity training or real-world cybersecurity expertise. Cataloguing, information retrieval, user services, and knowledge organization have historically been the main topics of LIS curricula. Many LIS instructors find cybersecurity to be outside of their academic comfort zone because it is a more technical and quickly changing field. As a result, if instructors lack the necessary competence, courses may be shallow or irrelevant. Cross-departmental

cooperation or adjunct professors may be relied upon, which may not be reliable or sustainable. Current faculty members must engage in ongoing professional development, but there are frequently few incentives and chances for this kind of upskilling.

Curriculum Strictness and Requirements for Accreditation (such as NUC Guidelines): National bodies like the National Universities Commission (NUC) influence LIS curricula in Nigeria and other controlled academic settings. Although these rules are meant to promote uniformity, they may provide challenges when introducing new or multidisciplinary topics, such as cybersecurity: Revisions to curricula frequently undergo drawn-out bureaucratic procedures that might not keep up with the rapidly evolving demands of cybersecurity. With little freedom to add additional electives or specialty modules, LIS programs may be restricted to typical course plans. There can be a discrepancy between the competencies allowed by the current curriculum structure and those needed in the digital information world.

Funding and Infrastructure Restrictions: Many LIS departments lack the specific infrastructure needed for cybersecurity instruction. For practical experience and hands-on learning, this includes network settings, simulation software, safe servers, and technical labs. licenses for threat detection systems, firewalls, and forensic software, among other cybersecurity solutions. Long-term financing for curriculum enrichment, staff training, and digital infrastructure improvements through outside alliances or certifications (e.g., CompTIA Security+, CISSP).

The incorporation of cybersecurity education is made more difficult in many schools by the restricted funding allotted for LIS programs, particularly when traditionally STEM-focused departments are given precedence.
Interdisciplinary Collaboration: Forming alliances with divisions such as information technology or computer science might aid in closing the knowledge gap, but doing so calls for institutional cooperation and resource sharing.

Market Relevance and Employability for Graduates: Information professionals with a working knowledge of cybersecurity are in more demand. LIS graduates may become less competitive in the changing digital economy if cybersecurity is not integrated.

Ethical and Legal Aspects: In order to be in line with professional principles such user confidentiality, intellectual freedom, and information access, LIS education must also incorporate the ethical, legal, and privacy aspects of cybersecurity.

A deliberate, phased strategy that incorporates faculty development, curriculum flexibility, outside collaboration, and proactive lobbying within the university system and accreditation authorities is necessary to overcome these obstacles.

RECOMMENDATIONS AND THE WAY FORWARD

Partnerships with cybersecurity experts and organizations must be promoted: There are four ways to accomplish this. i. through institutional cooperation LIS schools ought to form strategic alliances with cybersecurity specialists, non-governmental organizations, government ICT agencies (like NITDA and NCC), and business titans like ISACA Nigeria and CSEAN (Cyber Security Experts Association of Nigeria); ii. through industry exposure and guest lectures. Here, cybersecurity

specialists can be asked to provide case studies, workshops, and practical sessions as visiting experts or adjunct lecturers; iii. internship and mentorship programs. This can be accomplished by encouraging LIS students to participate in mentorship and internship programs at cybersecurity-related firms, which will expose them to real-world threats and applications; and iv. collaborative curriculum development. Course contents can be co-developed and review modules with cybersecurity practitioners to ensure relevance and applicability to emerging trends and threats.

Suggested Phases of Curriculum Integration

Phase 1: Foundation Awareness Courses: In this phase, fundamental cybersecurity knowledge can be introduced as an elective in general studies on its own or as part of information literacy courses. Online safety, data protection concepts, password management, and typical cyberthreats are a few possible subjects.

The second phase, Intermediate and Applied Courses, may see the launch of cybersecurity courses specifically tailored to LIS, such as "Cybersecurity for Information Professionals" or "Digital Safety and Risk Management in Libraries." Data governance, digital preservation concerns, safe information systems, and ethical information management should all be prioritized.

Phase 3: Advanced Specialization Tracks: This phase can take into account the creation of optional advanced modules for postgraduates or final-year students, such as ICT Law and Policy in Information Institutions, cyber-Forensics in Libraries and Archives, and information risk management. It can also promote thesis and project work centered on cybersecurity topics in LIS contexts.

Faculty Development Programmes

Programs for faculty development may, but shouldn't be restricted to:
Workshops for Capacity Building: In this area, LIS educators can frequently participate in national training sessions on cybersecurity principles, trends, and instructional strategies.

Sponsorship for Certifications: To increase their confidence and authority in teaching cybersecurity, faculty members can be given the chance to obtain cybersecurity certifications (such as CompTIA Security+, CISSP, and CISA).

Curriculum Design Training: In accordance with NUC accreditation criteria and norms, the curriculum committee can receive training on incorporating cybersecurity into LIS frameworks.

Academic Exchange and Fellowships: Here, LIS academic members can be offered sabbaticals or fellowships to work or study in cybersecurity-rich areas both domestically and abroad.

According to the aforementioned, graduates of Nigerian LIS programs can be both literate in information system management and robust in the face of the increasing cybersecurity threats that libraries and information institutions confront in the digital age.

CONCLUSION AND FUTURE RESEARCH DIRECTIONS

Conclusion

The urgent necessity to incorporate cybersecurity into Nigeria's Library and Information Science (LIS) curriculum has been brought to light by this narrative review. Information systems are now more susceptible to cyberattacks due to the changing digital environment in which libraries function, which calls for a change in the way LIS professionals are taught. The literature's main conclusions point to a large curriculum deficit in cybersecurity competencies in Nigerian LIS education. Institutional constraints like strict curricular frameworks, a shortage of faculty experience, and insufficient infrastructure support are also highlighted in the review. Crucially, by training graduates who can protect digital assets, guarantee information integrity, and assist with national digital transformation initiatives, LIS plays a critical role in fostering secure information ecosystems. As frontline information managers, librarians and information professionals must now be equipped not only with technical knowledge but also with strategic cybersecurity awareness that aligns with global best practices.

Future Research Directions

In order to expand on the knowledge gained from this review, the following areas need empirical research:

Assessments of Stakeholder Readiness: Studies should look into how ready and willing LIS departments, instructors, students, and institutional leaders are to embrace cybersecurity topics. This include evaluating attitudes, perceived impediments, and current competencies.

Pilot Curriculum Implementation: Research on the viability, efficacy, and student results of experimental studies or pilot programs that add cybersecurity courses into particular LIS schools can be very helpful.

Industry-LIS Collaboration Models: Examine the efficacy of several collaboration approaches between cybersecurity experts and LIS departments, emphasizing knowledge transfer, sustainability, and curriculum co-design.

Faculty Capacity Development Needs: To complement cybersecurity instruction, surveys or interviews with LIS educators can be used to pinpoint specific professional development requirements.

Effect on Employability: The effects of cybersecurity-integrated LIS programs on graduate employability, professional relevance, and career diversity can be assessed through longitudinal research.

Future research might provide useful frameworks for curriculum change by taking into account the aforementioned research gaps. This would guarantee that LIS education in Nigeria stays robust, relevant, and responsive to the information security concerns of the twenty-first century.

Conflict of Interest

There is no conflict of interest or whatsoever regarding this paper. The paper is the original idea of the author.

References

Abrahams, T., Farayola, O., Kaggwa, S., Uwaoma, P., Hassan, A., & Dawodu, S., (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. *Computer Science & IT Research Journal*, 5(1), 100-119. 10.51594/csitrj.v5i1.708.

Abubakara, B.M. (2021). Library and Information Science (LIS) education in Nigeria: emerging trends, challenges and expectations in the digital age. *Journal of Balkan Libraries Union,*8(1), 57-67.

Adejumo, F., Oye, E., & Olorunleke, P. (2015). A critical examination of the librarian's registration council of Nigeria code of ethics in the light of international best practices in Library and Information Science Professions. *Library Philosophy and Practice (e-journal)*,1281. http://digitalcommons.unl.edu/libphilprac/1281

Agwu-Okoro, N.G. (2025). Cybersecurity strategies for startups. https://www.linkedin.com/pulse/data-protection-cybersecurity-strategies-startups-agwu-okoro-joczf

Ahmed, B., & Ahmed, A.B. (2024). Influence of Information and Communication Technology (ICTs) in libraries for information service delivery: issues and practices. *Jewel Journal of Librarianship,* 19(1), 12-22.

Ahamed, B., Polas, M.R.H., Kabir, A.I., Sohel-Uz-Zaman, A.S.M., Al-Fahad, A., Chowdhury, S., & Dey, M.R. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: the role of cybersecurity attitude in the 4.0 industrial revolution era. *SAGE Open*, 1–14, DOI: 10.1177/21582440241228920

Alliance Law Firm, ALF (2025). Cybersecurity In the Nigerian Energy Sector. https://alliancelawfirm.ng/cybersecurity-in-the-nigerian-energy-sector/

Alliance Law Firm (2024). Compliance with the Nigeria Data Protection Act 2023 (NDPA): outlook for 2024. https://www.lexology.com/library/detail.aspx?g=b6e44c8c-64a9-4585-ba83-a010b96787c8#:~:text=2,with%20Requisite%20Skill%20and%20Expertise

Ayo-Odewale, B. (2023). NUC introduces software engineering, cybersecurity, others to university curriculum. https://technext24.com/2023/09/01/nuc-tech-nigeria-courses/?utm_source=chatgpt.com

Bakrin, S.M., Bello, M.A., & Ogunrinde, M.A. (2020). Adoption of Cloud Computing and OPAC Visibility in Nigerian University Library System. *International Journal of Information Science and Management,* 18(2), 133-149.

Bellini, E. and Tammaro, A.M. (2024). Cybersecurity for digital libraries: an interview with Emanuele Bellini. *Digital Library Perspectives, 40 (2), 348-355. https://doi.org/10.1108/DLP-05-2024-147*.

Catholic University of America (2025). Digital libraries. https://lis.catholic.edu/academics/courses/course-descriptions/index.html https://lis.catholic.edu/academics/courses-of-study/digital-libraries/index.html

Crick, T., Davenport, J. H., Irons, A., & Prickett, T. (2019). A UK Case Study on Cybersecurity Education and Accreditation. *ArXiv*. https://arxiv.org/abs/1906.09584

Chaudhary, S., Gkioulos, V., & Sokratis, K. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review,* 50, 100592, https://doi.org/10.1016/j.cosrev.2023.100592.

Chukwumaobi, N.J. (2018). assessment of the practice of preserving digital materials in university libraries in South-east, Nigeria. A Dissertation, Nnamdi Azikiwe University, Awka.

Nigerian Data Protection Act (2023). Explanation memorandum. https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf

Dahiru, S. (2022). Reinvigorating Nigerian Library and Information Science (LIS) Curriculum to Cope with Dwindling Job opportunities and Latest Technological Advancement. 2022 Library and Information Science Conference (LISCON) 2022, University of Ibadan, Nigeria. https://theliscon.org/category/proceedings/2022/

D'Amato, L. (2025). Resource sharing that expands library collections and delivers fast—some e-resources in 15 minutes. https://www.oclc.org/en/worldshare-ill.html

Dasuki, M.S. (2014). National cybersecurity policy. https://sherloc.unodc.org/cld/uploads/res//treaties/strategies/nigeria/nga0001s_html/NATIONAL_CYBESECURITY_STRATEGY.pdf

Diesch, R., Pfaff, P., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, 92, 101747, https://doi.org/10.1016/j.cose.2020.101747.

Dunmade, A.O. & Tella, A. (2023). Libraries and librarians' roles in ensuring cyberethical behaviour. *Library Hi Tech News*, 40 (7), 7-11. https://doi.org/10.1108/LHTN-04-2023-0068

Ebelogu, C.U., Prasad, R., Bisallah, H.I., Hammawa, B.M., & Musa, I. (2025). Investigation of cybersecurity vulnerabilities and mitigation strategies in nigeria's oil and gas industry. *ABUAD Journal of Engineering and Research Development*, 8(1), 140–150. DOI: https://doi.org/10.53982/ajerd.2025.0801.15-j

Fatade , A. T., Ajiboye , B. A., & Ogunjimi, M. S. I. (2023). Disaster preparedness and security management in two academic libraries in South-West Nigeria. Gateway Information Journal, 24(1 & 2), 46–61. Retrieved from https://www.gatewayinfojournal.org/index.php/gij/article/view/35

Familoni, B.T. & Shoetan, P.O. (2024). Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. *Computer Science & IT Research Journal*, 5(4):850-877 DOI:10.51594/csitrj.v5i4.1046

Elebiju, O. (2024). Digital disconnects? Unpacking the extent and limits of engagement with the digital TV switchover among remote rural communities in the Lagos region. A Thesis submitted for the award of degree of Doctor of Philosophy University of Stirling, Faculty of Arts and Humanities.

Ezema, A.L., Ogbuabor, C.D., & Ekenna, U.C. (2023). Operational challenges of library and information science education in a digital environment. *Library and Information Science Digest* 17(1), 16-28.

IFLA (2022). IFLA Statement on cybersecurity approved by the IFLA Governing Board, February 2022. https://repository.ifla.org/server/api/core/bitstreams/ade7b283-522d-4a45-bca5-5fcb552e62b2/content#:~:text=Governments%20should%3A%20%E2%97%8F%20Ensure%20that,of%20Disinformation%20as%20a%20Cybersecurity

IFLA (2025). IFLA statement on privacy in the library environment. https://www.ifla.org/publications/ifla-statement-on-privacy-in-the-library-environment/

George, M. (2025). GDPR Compliance: your guide to European data privacy regulations. https://www.ketch.com/regulatory-compliance/general-data-protection-regulation-gdpr

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*, *35*(1-2), 89-103. https://doi.org/10.1177/09557490251335954

Ikwuanusi, U., Adepoju, P., & Odionu, C (2023). Advancing ethical AI practices to solve data privacy issues in library systems. *International Journal of Multidisciplinary Research Updates*, 6(2), 033-044. 10.53430/ijmru.2023.6.1.0063.

Igbinovia, M. & Clifford, I. (2023). Cyber security in university libraries and implication for library and information science education in Nigeria. *Digital Library Perspectives*, 39(3), 10.1108/DLP-11-2022-0089.

Igwe, U. (2021). Nigeria's growing cybercrime threat needs urgent government action. https://blogs.lse.ac.uk/africaatlse/2021/06/09/nigerias-growing-cybercrime-phishing-threat-needs-urgent-government-action-economy/

Jegbefume, C.M., Ikhimeakhu, D.S., & Muhammed, A. (2025). Curriculum development in library and information science in Nigeria in the era of technology advancement: challenges and expectations. *Jewel Journal of Librarianship*, 20(1), 1-8.

Kwanya, T., Kibandi, I.M., & Gatiti, P. (2024). Re-imagining library and information services in the digital era. Proceedings of the 26th Standing Conference of Eastern, Central and Southern African Library and Information Associations (SCECSALXXVI) held on 22nd — 26th April, in Mombasa, Kenya

Lawal, S. (2024). Cybersecurity threats in Nigeria: prevention and response. https://osundefender.com/cybersecurity-threats-in-nigeria-prevention-and-response/

Mugwisi, T. & Mugwisi, T. (2024). Investigating the integration of ICTs in Library and Information Science (LIS) curriculum in Zimbabwe. *Library Philosophy and Practice* (e-journal). 8035. https://digitalcommons.unl.edu/libphilprac/8035

Muhusina Ismail, Nisha Thorakkattu Madathil, Meera Alalawi, Saed Alrabaee, Mohammad Al Bataineh, Suhib Melhem, Djedjiga Mouheb. (2024). Cybersecurity activities for education and curriculum design: A survey. *Computers in Human Behavior Reports,* 16, 100501, https://doi.org/10.1016/j.chbr.2024.100501.

Nadeem, A. (2023). Cybersecurity as a Crosscutting Concept Across an Undergrad Computer Science Curriculum: An Experience Report. ArXiv. https://doi.org/10.1145/3626252.3630821

Nakiyingi, R.L. (2024). Strengthening Cybersecurity in Nigerian libraries: challenges, mitigation strategies, and future trends. *Research Output Journal of Biological and Applied Science*, 3(2),23-27.

NUC (2014). Benchmark minimum academic standards for undergraduate programmes in Nigerian universities. https://nuc.edu.ng/wp-content/uploads/2015/09/Education%20Draft%20BMAS.pdf#:~:text=education%20for%20Library%20and%20Information,for%20all%20types%20of%20libraries

Nigerian Communication Commission, NCC. (2024). Baseline Study on the Level of Digital Skills in Nigeria (Women, Youth, and the Physically Challenged) (RD-1). https://www.ncc.gov.ng/sites/default/files/2024-11/Baseline-Study-on-Level-of-Digital-Skills-on-Nigeria-%28Women%2C-Youth-and-the-Physically-Challenged---RD1.pdf

Obim, I.E. & Akpokurerie, A.O. (2023). Awareness of cybersecurity and its impact on information storage in the university libraries in south east Nigeria. *Information Technology and Librarianship*, 3(2), 126-140.

Ocks, Y. & Salubi, O.G. (2024). Privacy Paradox in Industry 4.0: A review of library information services and data protection. *South African Journal of Information Management*, 26(1), a1845. **https://doi.org/10.4102/sajim.v26i1.1845**

Ogene, F. (2024). Cybersecurity and IT governance challenges in Nigeria: strategic investment needs and the path forward for a resilient digital economy. *International Journal of Computer Applications*, 186(55), 41-46.

Okeji, C.C. & Mayowa-Adebara, O. (2021). An evaluation of digital library education in library and information science curriculum in Nigerian universities. *Digital Library Perspectives*, 37(2), 102-118. https://doi.org/10.1108/DLP-04-2020-0017

Okpara, H.U., Alegbeleye, G.O, Babalola, O.Y. (2024). Organisational justice and librarians' digital security behaviours in universities in south-east, Nigeria. *International Journal of Education, Library and Information Communication Technology,* 3(1), 32-42.

Okusi, O. (2024). Cyber security techniques for detecting and preventing cross-site scripting attacks. *World Journal of Innovation and Modern Technology*, 2(1), 71-89. DOI:10.56201/wjimt.v8.no2.2024.pg71.89

Omoike A. & Alabi, R. (2023). Awareness and perception of cybersecurity among librarians in federal universities in South-West, Nigeria. Journal of Library Services and Technologies, 5(3), 90 – 104. DOI: http://doi.org/10.47524/jlst.v5i3.91

One Trust DataGuide (2020). Comparing privacy laws: GDPR v. Nigeria data protection regulation https://www.dataguidance.com/sites/default/files/gdpr_v._nigeria.pdf

Oladosu, S. (2024). Curriculum Development and Inclusion of Network Security in Nigeria's Education System. EduGist. https://edugist.org/curriculum-development-and-inclusion-of-network-security-in-nigerias-education-system/?utm_source=chatgpt.com

Oladokun, B.D., Oloniruha, E.A., Mazah, D., & Okechukwu, O.O. (2024). Cybersecurity risks: a sine qua non for university libraries in Africa. *Southern African Journal of Security* 2(1), 1-14.

Osaro, M. & Osazuwa, C. (2024). Confidentiality, integrity, and availability in network systems: a review of related literature. *International Journal of Innovative Science and Research Technology,* 8(12), 1946-1955.

Oloruntade, G. (2024). 03: Can 3MTT turn Nigeria into a global tech talent powerhouse? https://techcabal.com/2024/10/04/3mtt-nigeria-tech-talent-powerhouse/#:~:text=After%20she%20was%20selected%2C%20Aliyu,foundational%20concepts%20in%20their%20chosen

Oyelude, A.A. (2023). Teaching Digital Preservation and Curation in Library and Information Science Schools: The State of the Art in Nigeria. *88th IFLA World Library and Information Congress* (WLIC), 2023 Rotterdam; https://repository.ifla.org/handle/20.500.14598/2693.

Panteli, N., Nthubu, B.R. & Mersinas, K. (2025). Being responsible in cybersecurity: a multi-layered perspective. *Information System Front*ier, https://doi.org/10.1007/s10796-025-10588-0

Pinki, I. (2024). Data Analytics and LIS Education. *VEETHIKA-An International Interdisciplinary Research Journal*, 10(3), 42-48. DOI:10.48001/veethika.2024.10.03.005

Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2023). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions, *Blockchain: Research and Applications*, 5(2), 100178, https://doi.org/10.1016/j.bcra.2023.100178.

Robert Gordon University (2025). Module Database Search – Digital libraries. http://www4.rgu.ac.uk/prospectus/modules/disp_moduleView.cfm?Descriptor=CBM836&Revision=1

Reddy, A.N.M. (2024). Librarianship in the Age of Artificial Intelligence (AI) DOI:10.13140/RG.2.2.10509.04322. Conference: BOSLA-SNDT Women's University Special Lecture.

Saha, R. (2024). Data privacy and cyber security in digital library perspective: safe guarding user information. *International Journal of Scientific Research in Engineering and Management, 08(04).* DOI:10.55041/IJSREM30761

Sahabi, M.K & Otobo, E.E (2021) Academic library and challenges of service delivery in nigerian universities in the digital era. information impact: *Journal of Information and Knowledge Management,* 12:2,51-61, DOIhttps://dx.doi.org/10.4314/iijikm.v12i2

Singh, K., Chatterjee, S., Mariani, M., & Wamba, M.F. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic

changes in the macroeconomic business environment. *Technovation,* 143, 103219, https://doi.org/10.1016/j.technovation.2025.103219.

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *MDPI Electronics 11*(14), 2181 DOI:10.3390/electronics11142181

TechTrends (2023). NUC Adds Cybersecurity Software Engineering, Others to Nigerian University Curriculum. https://techtrends.africa/nuc-adds-cybersecurity-software-engineering-others-to-nigerian-universitycurriculum/#:~:text=During%20a%20recent%20stakeholder%20meeting%2C,implemented%20beginning%20in%20September%202023

University of Washington (2025). Course description. https://www.washington.edu/students/crscat/imt.html

University of Pretoria (2025). MIT ICT Information Science (code 12254016). https://www.up.ac.za/school-of-information-technology/article/1906037/mit-ict-information-science-code-12254016

Weitzenboeck, E.M., Lison, P., Cyndecka, M., & Langford, M. (2022). The GDPR and unstructured data: is anonymization possible?, *International Data Privacy Law*, 12(3), 184–206, https://doi.org/10.1093/idpl/ipac008

Wells, D. (2021). Online Public Access Catalogues and library discovery systems. *Knowledge Organization* 48(6), 457-466. 104 references. DOI:10.5771/0943-7444-2021-6-457.

Appendixes

Appendix 1

Proposed Module: Cybersecurity in Library and Information Science

This course module gives librarians the information and abilities they need to safeguard library patrons, data, and systems. It incorporates theory and practice and builds on Nigeria's educational goals (such as NUC's emphasis on ICT in LIS, NUC 2015; NUC, 2024). Each level—undergraduate, postgraduate, and professional—covers pertinent laws (such as the Nigeria Data Protection Act 2023, Cybercrimes Act, and FOI Act) and places an emphasis on ethics, incident response, and practical exercises in accordance with NUC accreditation criteria. Understanding data privacy laws, creating security policies, and handling cyber events in library settings are important learning objectives (Nikiyingi, 2024).

Undergraduate Module (e.g., 3-credit course)

Title: *Information Security and Cybersecurity in Libraries*

Description: Students studying libraries are introduced to information security concepts in this subject. Nigeria's data security regulations (NDPA 2023, Cybercrimes Act 2015), common cyberthreats (virus, phishing, ransomware), the CIA triad (Confidentiality, Integrity, Availability), and professional ethics (patron privacy, intellectual freedom) are among the topics covered. The course blends theoretical lectures on topics like security policy and regulatory requirements with hands-on laboratories on topics like basic firewall configuration and risk assessment. Students will be able to deploy security controls to library systems and comprehend their ethical responsibilities to safeguard user data by the conclusion of the semester.

Learning Objectives and Outcomes: Students will be able to:

- **Explain** fundamental cybersecurity concepts and threats in libraries.
- **Identify** and summarize Nigeria's key information security laws (Data Protection Act 2023, NDPR, Cybercrimes Act, FOI Act) and their relevance to libraries.
- **Apply** basic security measures (access controls, encryption, backups) to protect library data and IT resources.
- **Demonstrate** knowledge of ethical issues (patron privacy, intellectual freedom) and professional codes, ensuring patron data protection.
- **Develop** a simple incident response plan (steps for detection, containment, recovery) for a hypothetical library cyber-incident.
- **Work collaboratively** on case studies to practice problem-solving (e.g. responding to a ransomware attack or data breach).

Weekly Breakdown (sample 14-week semester):

- **Introduction to Library Cybersecurity:** Role of technology in libraries; CIA triad; security goals. (Aligns with NUC's ICT focus)
- **Nigeria Data Protection Act 2023 & NDPR:** Overview of NDPA 2023 objectives; data subjects' rights; consequences of non-compliance.

- **Cybercrimes Act 2015 & FOI Act 2011:** Key provisions on hacking, fraud, privacy; FOI's implications for public libraries.
- **Threat Landscape – Malware & Phishing:** Types of attacks (viruses, ransomware); case studies of library incidents.
- **Network Security Basics:** Firewalls, antivirus, secure Wi-Fi in library settings; hands-on lab.
- **Access Control & Authentication:** Password policies, multi-factor authentication (MFA); ethics of user accounts.
- **Data Backup and Recovery:** Backup strategies; recovery drills; case studies emphasizing backups and incident response.
- **Ethical and Professional Issues:** Patron confidentiality; IFLA/Nigerian library ethics (e.g., duty to protect user data).
- **Security Policies & Governance:** Writing a library security policy; roles of librarians and administrators.
- **Incident Response Planning:** Steps in an incident response plan; forming response teams as in real cases.
- **Physical Security & Human Factors:** Securing equipment; social engineering awareness; staff training importance.
- **Emerging Issues:** Cloud security, IoT in libraries, cybersecurity awareness.
- **Case Study Workshop:** Student presentations on assigned incidents (e.g. leaked patron data, DDoS attack).
- **Review & Integration:** Integrating technical controls, legal compliance, and ethics in library cybersecurity.

Teaching Methods and Assessment:

- **Lectures** and **seminars** to cover theory and laws (NDPA, Cybercrimes Act).
- **Hands-on labs** (e.g., configuring firewalls, simulating malware response) to build practical skills.
- **Group projects/case studies** (weekly or multi-week) to analyze real-world scenarios and develop response plans.
- **Guest lecture or workshop** by a data protection expert (NDPC official or IT specialist).
- **Assessments:** Quizzes on legal provisions and concepts; a written incident response plan; a final exam; group project report and presentation.

Readings and Policy Documents:

- **Nigeria Data Protection Act 2023** (official text).
- **Nigeria Data Protection Commission (NDPC) Guidelines** (e.g., GAID 2025).
- **Cybercrimes (Prohibition, Prevention etc.) Act, 2015** (excerpts).
- **Freedom of Information Act, 2011** (relevant sections on data access).
- **IFLA/ALA Code of Ethics** for librarians (on privacy and freedom of access).

- **Introductory textbook** on information security (e.g., Stallings & Brown, *Computer Security: Principles and Practice*).
- **Selected articles**: Nakiyingi et al., "Strengthening Cybersecurity in Nigerian Libraries" (2024); Igbinovia & Ishola (2023) on cybersecurity education in Nigerian LIS.
- **NUC BMAS for Library Science** (to show alignment).

Appendix 2

Postgraduate Module (e.g., Master's specialization)

Title: *Advanced Information Security and Risk Management for Libraries*

Description: This seminar-style course deepens understanding of cybersecurity governance in libraries and information centers. It covers advanced topics: security management frameworks (ISO 27001, NIST), risk assessment models, cryptography basics, digital forensics, and emerging technologies (AI, blockchain) in security. Emphasis is on research, policy development, and leadership: students critique national policy (e.g., NDPA 2023 and NCPS 2021), design institutional security strategies, and explore ethical dilemmas (e.g., balancing open access vs. confidentiality). The course is largely discussion and project-driven, preparing graduates to lead security initiatives in complex information environments.

Learning Objectives and Outcomes: Students will be able to:

- **Evaluate** security frameworks (e.g., ISO/IEC 27001, National Cybersecurity Policy) and propose library-specific security governance.
- **Conduct** risk assessments for library IT systems and recommend controls (encryption, IDS/IPS, network segmentation).
- **Analyze** Nigeria's data protection landscape (NDPA 2023, NDPR 2019, GDPR comparisons) and assess institutional compliance requirements.
- **Apply** incident response and digital forensics methods (e.g., evidence handling) in case simulations.
- **Investigate** emerging challenges (e.g., insider threats, IoT, cloud) and propose innovative mitigation (e.g., AI-based monitoring, blockchain for integrity).
- **Advance** the discourse on library security by reviewing recent research (e.g., Nakiyingi et al., 2024) and contributing to policy discussions.

Weekly/Topical Breakdown (12–14 weeks):

- **Security Governance in Libraries:** Leadership roles; creating a security culture; staff training programs.

- **Standards and Frameworks:** ISO 27001/27002 overview; adapting international standards to libraries.
- **Risk Assessment & Management:** Threat modeling for library assets; conducting vulnerability assessments.
- **Legal and Regulatory Review:** In-depth study of NDPA 2023 (especially sections on breaches/penalties), GDPR overview; institutional data classification.
- **Digital Forensics and Incident Response:** Evidence gathering; building IR teams (case study of [14]), reporting incidents to NDPC.
- **Network & Systems Security:** Advanced topics (segmentation, VPNs, wireless security in campuses).
- **Cryptography and Access Control:** Basics of encryption, PKI, secure authentication for library services.
- **Ethics and Information Rights:** Privacy vs. access debates; case studies on ethical leaks or censorship.
- **Cloud and New Technologies:** Securing cloud-based ILS; IoT devices (smart labs) security.
- **Disaster Recovery and Business Continuity:** Developing disaster plans; ensuring service continuity (e.g., offsite backups).
- **Cybersecurity Research Methods:** Planning LIS security research; reviewing literature (e.g., Igbinovia & Ishola 2023).
- **Student Presentations:** Research projects on topics like mobile device security in academic libraries, or compliance auditing.
- **Policy and Strategy Workshop:** Drafting a library cybersecurity policy (mock accreditation review).
- **Summary & Future Trends:** Review of AI, blockchain, awareness campaigns for librarians.

Teaching Methods and Assessment:

- **Seminars and discussions** (graduate-level, focusing on critical analysis).
- **Case study research:** Students analyze high-profile incidents (global or local) and report lessons learned.
- **Project/paper:** Each student undertakes a small research project or policy proposal related to library cybersecurity.
- **Presentations:** Students present on specialized topics (e.g., “Implementing ISO 27001 in our University Library” or “Cybersecurity Certification for Librarians”).
- **Assessment:** Graded on research paper quality, seminar participation, case analysis write-ups, and a final exam covering legal and strategic aspects.

Readings and Resources:

- **Academic articles:** E.g. Igbinovia & Ishola (2023), Nakiyingi et al. (2024), and others on library security (emerging tech, ethics).

- **International standards:** ISO/IEC 27001, NIST Cybersecurity Framework (selected readings).
- **Government documents:** Nigeria's National Cybersecurity Policy and Strategy (NCPS 2021), NDPC GAID 2025.
- **Books:** Advanced texts on information security management.
- **Guidelines:** NDPC guidelines for public institutions, IFLA Statements on Privacy.

Appendix 3

Professional Development Workshop (e.g., Continuing Education Short Course)

Title: *Cybersecurity Essentials for Library Professionals* (short course/certificate)

Description: A concise (e.g., 2–3 day or 4-week evening) program for current librarians and information staff. Covers practical fundamentals: recognizing cyber threats, complying with NDPA 2023, basic risk controls, and ethical responsibilities. Emphasis is on immediate workplace application: participants learn to update library security policies, conduct mini-risk audits, and respond to incidents. The workshop combines lectures, group discussions, and hands-on exercises (e.g., configuring secure library PCs, drafting user-data privacy notice).

Objectives and Outcomes: By course end, participants will:

- **Recognize** common cybersecurity threats to libraries (phishing emails, malware, insider risks).
- **Understand** their obligations under Nigeria's data protection and cybercrime laws, and how these affect library operations (Nikiyingi, 2024).
- **Implement** basic security measures (strong passwords, secure Wi-Fi, regular backups) in their libraries.
- **Apply** an ethical framework: respect patron confidentiality and use data responsibly.
- **Develop** a simple incident response checklist and know when/how to escalate issues (e.g., notifying NDPC of a breach).
- **Collaborate** with peers to share best practices and update library manuals.

Topics/Schedule:

- **Introduction & Threat Overview:** Why library cybersecurity matters; local examples.
- **Legal Responsibilities:** Summary of NDPA 2023, Cybercrimes Act, FOI Act; patron data rights.

- **Practical Controls:** Demonstrations (setting up backups, secure logins); workshop on password managers.
- **Incident Response Drill:** Simulated breach exercise (phishing or ransomware scenario) and team response.
- **Ethics and Policy:** Group discussion on real-world dilemmas (e.g. handling confidential patron records).
- **Resource Review:** Overview of toolkits, NDPC resources, and where to find help.

Methods & Assessment:

- **Interactive lectures** with Q&A (focused and concise).
- **Hands-on practice:** e.g., configuring a firewall/router, using basic encryption tools.
- **Group exercises:** role-play for incident response; policy drafting in small teams.
- **Evaluation:** Participants complete a checklist or short quiz on key points; receive a certificate of completion.

Resources:

- **NDPC materials:** Handouts summarizing NDPA 2023 obligations, guides for public institutions.
- **Nigerian laws:** Excerpts from Cybercrimes Act and FOI Act (plain-language summaries).
- **Cybersecurity guides:** NIST tips or local frameworks adapted for librarians.
- **Selected articles:** Summaries of (Nakiyingi, 2024) or Igbinovia & Ishola (2023) to contextualize practices.
- **Online resources:** Links to NDPC webinars, free training (e.g., Cybersecurity 101).

Each module is designed to meet NUC's curricular goals and Nigeria's professional standards. The undergraduate and postgraduate modules align with NUC's BMAS for Library Science (e.g., ICT and information management competencies, NUC, 2015) and contribute to producing graduates globally competitive in data privacy and security. The professional course addresses national capacity needs, as identified by the Nigerian Data Protection Commission and library studies literature. Collectively, this curriculum ensures Nigerian LIS professionals are skilled in protecting library data and services while upholding ethical and legal standards.

About the author

Adeyinka Tella is a professor at Department of Library and Information Science, University of Ilorin, Ilorin, Kwara State Nigeria. He is a Research Fellow, at the University of South Africa, Pretoria, South Africa.