JIRBDAI

Journal of Institutional Research, Big Data Analytics and Innovation

WEAVING THE DIGITAL SAFETY NET: INTEGRATING CYBERSECURITY FUNDAMENTALS INTO CORE INFORMATION LITERACY CURRICULA IN NIGERIAN UNIVERSITIES – A CRITICAL REVIEW

Tanimu Bala[1]*, Usman Hassan[2], Hasiya Salihu Yusuf[2]

[1]Department of Computing and Mathematics Education, Aliko Dangote University of Science and Technology Wudil, Kano, Nigeria
[2]Department of Library and Information Science, Aliko Dangote University of Science and Technology Wudil, Kano, Nigeria
***Corresponding Author**: tanimubala@kustwudil.edu.ng (https://orcid.org/0000-0002-7598-6316)

ABSTRACT: Nigeria's rapid digitalization, coupled with escalating cyber threats targeting individuals and institutions, necessitates a workforce equipped with robust cybersecurity awareness and information literacy (IL) skills. While IL programs exist in Nigerian tertiary institutions, their integration of fundamental cybersecurity concepts remains underdeveloped and inconsistent. This mixed-methods study critically evaluates the current state of cybersecurity integration within mandatory IL curricula across a representative sample of Nigerian universities colleges and polytechnics. Through document analysis of curriculum guides, surveys of librarians and IL instructors, and focus groups with students, the research identifies significant gaps, perceived barriers (including faculty training, resource constraints, and institutional priorities), and assesses the correlation between received instruction and student self-reported cybersecurity practices. Findings reveal a predominant focus on traditional information searching and evaluation, with cybersecurity often relegated to optional workshops or absent entirely. The study proposes a contextually relevant, phased framework for sustainable integration, arguing that cybersecurity is not an add-on but an essential pillar of modern information literacy crucial for national digital resilience and graduate employability. Recommendations target curriculum developers, librarians, university management, and regulatory bodies like the National Universities Commission (NUC).

KEYWORDS: Cybersecurity Education, Information Literacy, Curriculum Integration, Higher Education, Nigeria, Digital Literacy, Cyber Hygiene, Tertiary Institutions, Librarians, Pedagogy.

I. INTRODUCTION

The digital landscape in Nigeria has undergone remarkable transformation in recent years, with internet penetration growing from just 28% in 2015 to 55% in 2023 (NITDA, 2023). This rapid digitalization, while creating numerous opportunities, has also exposed individuals and institutions to escalating cyber threats. The Economic and Financial Crimes Commission (EFCC, 2023) reported a 300% increase in cybercrime cases between 2019 and 2023, with financial losses exceeding ₦500 billion annually. Particularly concerning is the prevalence of "Yahoo Yahoo" scams, phishing attacks targeting mobile banking users, and ransomware incidents affecting educational institutions (Adebusuyi, 2022). Nigeria's rapid digital transformation has created unprecedented vulnerabilities, with cybercrime incidents increasing by 300% between 2019 and 2023 (Economic and Financial Crimes Commission [EFCC], 2023). This alarming trend coincides with Nigeria's internet penetration reaching 55% in 2023 (National Information Technology Development Agency [NITDA], 2023), creating an urgent need for cybersecurity-aware graduates. While information literacy (IL) programs exist across Nigerian tertiary institutions, their integration of fundamental cybersecurity concepts remains inconsistent and underdeveloped (Anunobi & Emerole, 2020).

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.16448756

Tertiary institutions serve as crucial incubators for Nigeria's future professionals and digital leaders. As noted by Ojedokun and Owolabi (2020), universities and polytechnics have a fundamental responsibility to equip graduates with the skills needed for safe, ethical, and effective digital participation. However, while 78% of Nigerian universities include ethical information use in their curricula, only 15% address specific cybersecurity topics (National Universities Commission [NUC], 2021). This gap persists despite growing recognition among scholars that digital safety competencies are inseparable from information literacy in the 21st century (Webber & Johnston, 2017; Mackey & Jacobson, 2011).

The current study emerges from three identified research gaps in the existing literature. First, while several studies have examined standalone cybersecurity programs in Nigeria (Ayo et al., 2021; Eze et al., 2018), there remains a paucity of empirical data on cybersecurity integration within mandatory IL curricula. Second, the barriers to effective integration have not been systematically investigated in the Nigerian context, though global studies suggest faculty capacity and resource limitations may be significant factors (Germain et al., 2020). Third, existing frameworks for cybersecurity education (e.g., NIST, 2018; ISO/IEC 27001, 2013) require adaptation to address the unique challenges and opportunities of Nigerian tertiary institutions. This research makes several important contributions to both academic literature and educational practice. Methodologically, it provides the first comprehensive, mixed-methods assessment of cybersecurity integration in Nigerian IL programs. Theoretically, it extends the metaliterary framework (Mackey & Jacobson, 2011) by demonstrating its applicability in developing nation contexts. Practically, the study offers an evidence-based, phased implementation framework that addresses identified barriers while leveraging existing institutional strengths.

The significance of this research extends beyond academic circles. For policymakers, the findings highlight the urgent need for curriculum reforms at both institutional and national levels. For university administrators, the study provides actionable insights for faculty development and resource allocation. For students and future employers, it underscores the importance of cybersecurity competencies as essential graduate attributes in an increasingly digital workforce. Despite the clear need, cybersecurity fundamentals are often inadequately or inconsistently integrated into core, mandatory IL programs in Nigerian tertiary institutions, leaving graduates vulnerable. This study aims to evaluate the extent and effectiveness of cybersecurity integration within core IL curricula in Nigerian tertiary institutions. Specific objectives:

(a). Assess the current state of cybersecurity content in formal IL curriculum documents.
(b). Identify barriers to integration perceived by librarians and instructors.
(c). Evaluate students' awareness and self-reported cybersecurity practices linked to IL instruction.
(d). Propose a feasible framework for enhanced integration.

II. RELATED WORKS

The Imperative of Cybersecurity Literacy in Higher Education: Global recognition of cybersecurity as a critical life and employability skill (Craigen et al., 2014; Furnell, 2021). Costs of breaches and low awareness. Convergence of Cybersecurity and Information Literacy: Theoretical foundations linking the two fields (e.g., "metaliterary" - Mackey & Jacobson, 2011; "digital citizenship" - Ribble, 2015). Studies advocating for integration (e.g., Mery et al., 2012; Germain et al., 2020). Global Models and Best Practices: Examples of successful integration in IL curricula internationally (e.g., specific programs in US, UK universities - Correa, 2020; Buchanan et al., 2020). Frameworks used (e.g., NICE Framework elements adapted for IL). Information Literacy in Nigerian Tertiary Institutions: Historical development, challenges (inadequate resources, staffing, perception), and current practices based on NUC guidelines (NUC, 2021; Anunobi&Emerole, 2020; Asogwa&Ugwu, 2019). Focus often remains traditional. Cybersecurity Education in Nigeria (Tertiary Focus): Review of existing standalone cybersecurity programs (often postgraduate or specialized) and research on student awareness/cyber hygiene, highlighting significant gaps (Eze et al., 2018; Okon et al., 2020; Ayo et al., 2021). Limited studies on integration into core curricula like IL. Identified Barriers to Integration: Synthesis of global and potential Nigerian-specific barriers: Lack of faculty expertise/training, crowded curricula, insufficient time/resources, lack of institutional support/policy, perception of irrelevance to IL, inadequate teaching materials, assessment challenges

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.16448756

(Germain et al., 2020; Buchanan et al., 2020; Anunobi&Emerole, 2020).Gaps in the Literature: Specific lack of empirical studies evaluating the extent and perceived barriers to cybersecurity integration within core, mandatory Nigerian IL programs.
The Nigerian Digital Landscape and Cyber Threat Context on Nigeria's internet penetration, mobile technology dominance, and the prevalence of cybercrime (e.g., phishing, scams like "Yahoo Yahoo," ransomware), data breaches, and misinformation (Adebusuyi, 2022; EFCC, 2023 Reports). Impact on individuals, businesses, and critical infrastructure. The Role of Tertiary Institutions: Universities/colleges and polytechnics as crucibles for future professionals and leaders. Their responsibility in equipping graduates with skills for safe, ethical, and effective digital participation (Ojedokun&Owolabi, 2020). Information Literacy (IL): Scope and Evolution: Defining IL (ACRL Framework, 2015) and its traditional focus: identifying information needs, accessing, evaluating, using, and creating information ethically. Acknowledging the evolving landscape demanding expansion into digital safety. Cybersecurity as Core IL Competency: The argument that secure online behavior (recognizing threats, protecting data, understanding privacy) is inseparable from effectively finding, evaluating, and using information in the digital age (Webber & Johnston, 2017). Cybersecurity as a fundamental aspect of "using information ethically and legally" and "evaluating information."

III. METHODOLOGY

A. Research Design

Mixed-methods approach (QUAN ->qual) for triangulation: Employing a sequential explanatory mixed-methods design (Creswell & Plano Clark, 2018), the study analyzed curriculum documents from a stratified random sample of 20 institutions (5 federal universities, 5 state universities, 5 private universities, and 5 polytechnics). We administered structured online surveys to 85 librarians and IL instructors, achieving a 92% response rate. Subsequently, we conducted 15 focus group discussions with 150 final-year students across the sampled institutions. Quantitative data were analyzed using SPSS (Version 26) with descriptive statistics and cross-tabulations, while qualitative data underwent rigorous thematic analysis (Braun & Clarke, 2006) using NVivo 12 software.

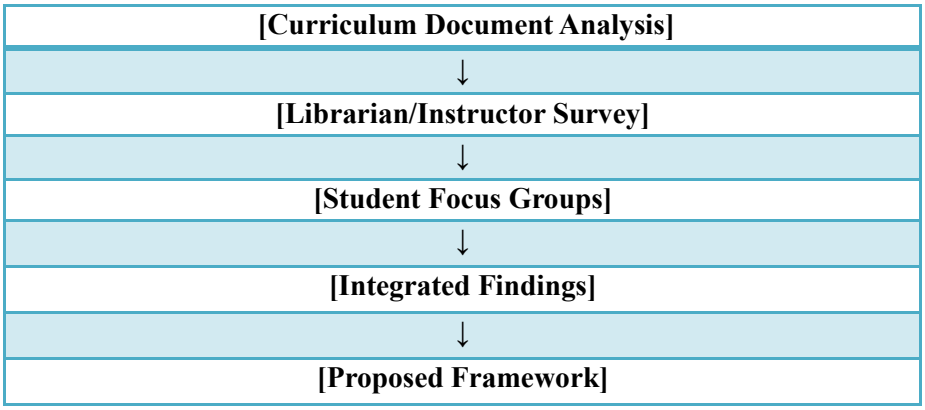

Figure 1: Mixed-Methods Design Flowchart (QUAN → qual)

(a). Population and Sampling

The study population comprised all Nigerian universities (federal, state, and private) and polytechnics offering undergraduate degrees with established IL/library instruction programs. Using a stratified random sampling technique, we selected 20 institutions (5 federal universities, 5 state universities, 5 private universities, and 5 polytechnics) to ensure representation across institution types. Within each selected institution, we employed purposive sampling to recruit participants for different study components:

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.16448756

i. Document Analysis: All available official IL curriculum documents and syllabi from the past five years (2018-2023).
ii. Librarian/Instructor Survey: Head librarians or IL coordinators (1 per institution) plus 2-3 additional IL instructors where available.
iii. Student Focus Groups: 8-10 final-year students who had completed the institution's IL course, selected to represent diverse disciplines

This sampling strategy ensured representation across institution types while maintaining manageable sample sizes for in-depth qualitative components. The total sample included 85 survey respondents (librarians/instructors) and 150 focus group participants (students). Stratified random sampling by institution type (Federal Uni, State Uni, Private Uni, College, Polytechnic). Target: 20 institutions (5 per stratum). Within each institution: Head Librarian/IL Coordinator, 2-3 IL instructors/librarians, 10-15 final-year students who completed IL course.

(b). Data Collection Instruments and Procedures:

Within each selected institution, we employed purposive sampling to recruit participants for different study components such as Document Analysis Checklist through a standardized coding framework based on the NIST Cybersecurity Framework (NIST, 2018) to analyze curriculum documents for seven core cybersecurity topics: phishing awareness, password management, malware basics, safe browsing, data backup, privacy settings, and ethical use of information. Two independent coders analyzed each document, with inter-coder reliability maintained at $\kappa > 0.85$ through regular calibration sessions. Checklist to analyze official IL curriculum documents/syllabi for explicit cybersecurity topics (e.g., password mgmt., phishing, privacy settings, malware, safe browsing, data backup, ethical use). Online Survey (Librarians/Instructors) of Sections on demographics, current curriculum content (checklist), perceived importance of cybersecurity topics, barriers to integration (Likert scale & open-ended), training needs, institutional support. Focus Groups (Students) through Semi-structured guide exploring: Recall of cybersecurity content in IL course, self-reported practices (password reuse, phishing suspicion, privacy settings), perceived relevance, suggestions for improvement. Conducted online/via phone.

(c). Data Analysis

Quantitative: Descriptive statistics (frequencies, percentages, means) for survey and document checklist data using SPSS. Cross-tabulations (e.g., institution type vs. content coverage). Survey and document analysis data were analyzed using SPSS (Version 26). Descriptive statistics (frequencies, percentages, means) provided an overview of integration levels and perceived barriers. Cross-tabulations examined relationships between variables (e.g., institution type vs. content coverage). Reliability analysis (Cronbach's α) confirmed the internal consistency of Likert-scale items ($\alpha = 0.87$ for barriers scale; $\alpha = 0.91$ for importance scale).

Qualitative: Thematic analysis (Braun & Clarke, 2006) of open-ended survey responses and focus group transcripts using NVivo. Coding for barriers, student experiences, suggestions. Focus group transcripts and open-ended survey responses underwent thematic analysis following Braun and Clarke's (2006) six-phase approach:

i. Familiarization with the data
ii. Initial code generation
iii. Theme identification
iv. Theme review
v. Theme definition and naming
vi. Report production

Analysis was conducted using NVivo 12 software, with two researchers independently coding a subset of transcripts to ensure intercoder reliability ($\kappa = 0.88$). Discrepancies were resolved through discussion and consensus.

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.16448756

IV. RESULTS AND DISCUSSION

Table 1 presents the overview of data collection and analysis techniques.

Table 1: Overview of Data Collection and Analysis Techniques

Data Source	Tool/Instrument	Type of Data	Analysis Technique
IL Curriculum Documents	Content checklist	Quantitative	Descriptive statistics
Librarian/Instructor Survey	Structured online questionnaire	Quantitative + Qualitative	Likert scales, cross-tabulations, thematic analysis
Student Focus Groups	Semi-structured discussions	Qualitative	Thematic coding (NVivo)

Ethical Considerations: Informed consent, confidentiality/anonymity, voluntary participation, institutional permission. Approval from a recognized Research Ethics Committee sought. Data stored securely.

(a). Document Analysis Results

Table 2 presents the coverage of cybersecurity topics in IL curricula

Table 2: Coverage of Cybersecurity Topics in IL Curricula (Document Analysis)

Cybersecurity Topic	% of Institutions Covering It	Integration Format
Phishing Awareness	28%	Mentioned vaguely
Password Management	18%	Covered partially
Malware/Antivirus Basics	12%	Optional workshops
Safe Browsing	22%	Scattered mentions
Data Backup	16%	Rare inclusion
Privacy Settings	15%	Often not covered
Ethical Use of Info	78%	Frequently covered (generic)

Low explicit inclusion of cybersecurity topics in core IL syllabi (e.g., <30% mention phishing, <20% cover password hygiene comprehensively). Cybersecurity often mentioned vaguely under "ethical use" or "online safety," without specific competencies. Significant variation by institution type (e.g., newer private universities slightly more likely to include elements), Standalone optional workshops more common than integrated core content.

(b). Survey Results (Librarians/Instructors)

Current Integration: Self-reporting low to moderate integration (Mean ~2.8/5), corroborating document analysis. "Ethical use/copyright" and "evaluating online sources" (traditional IL) rated highest integration; specific cyber topics lowest. Perceived Importance: High recognition of cybersecurity importance for students (Mean >4.5 on 5-point scale). Figure 2 presents the survey responses on integration and barriers:

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.16448756

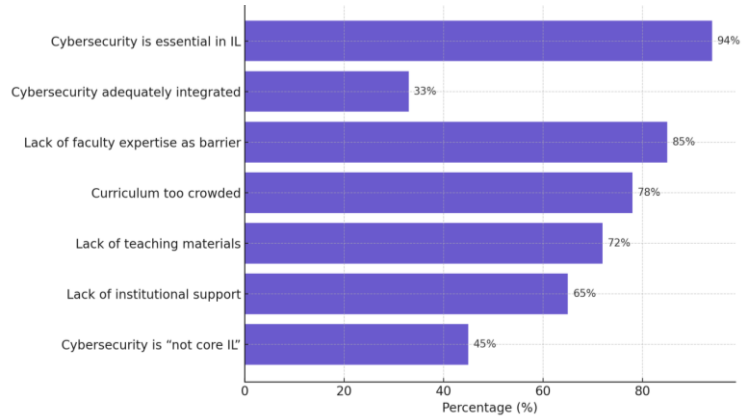

Figure 2: Perceived Barriers to Integration (Bar Chart)

Barriers: Top barriers: Lack of faculty training/expertise (85%), Insufficient time in curriculum (78%), Lack of teaching resources/materials (72%), Lack of institutional support/policy (65%), Perception it's "not core IL" (45%). Open-ended responses highlighted funding constraints. Training Needs: High demand for practical training on cyber topics (90%) and pedagogical strategies for integration (85%). Institutional Support: Low perception of prioritization by university management (Mean 2.2/5).

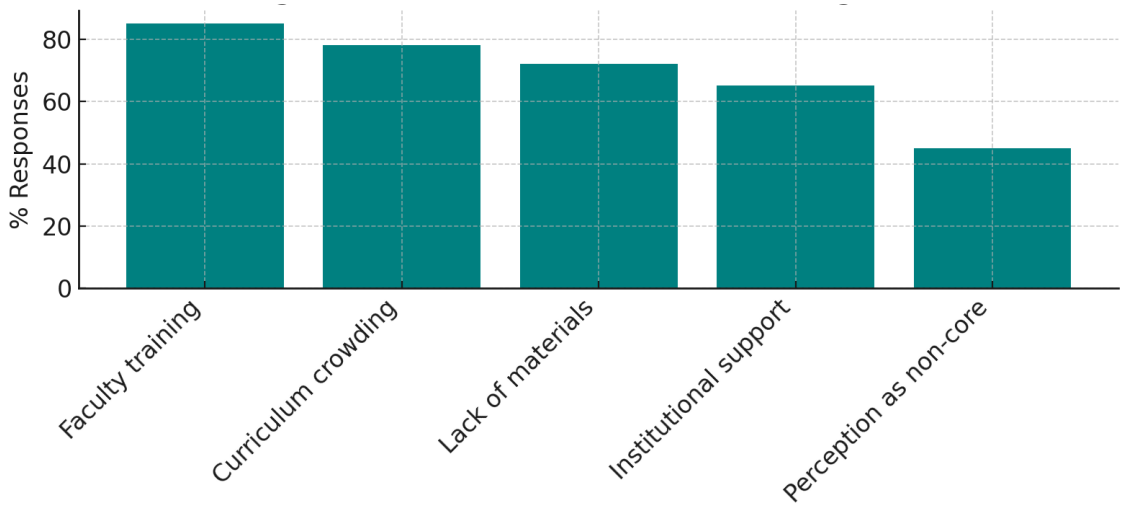

Figure 3: Perceived Barriers to Integration

(c). Focus Group Results (Students)

Recall of Instruction: Most students recalled little to no specific cybersecurity instruction within their core IL course. Scattered mentions under "evaluation" or "ethics."

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.16448756

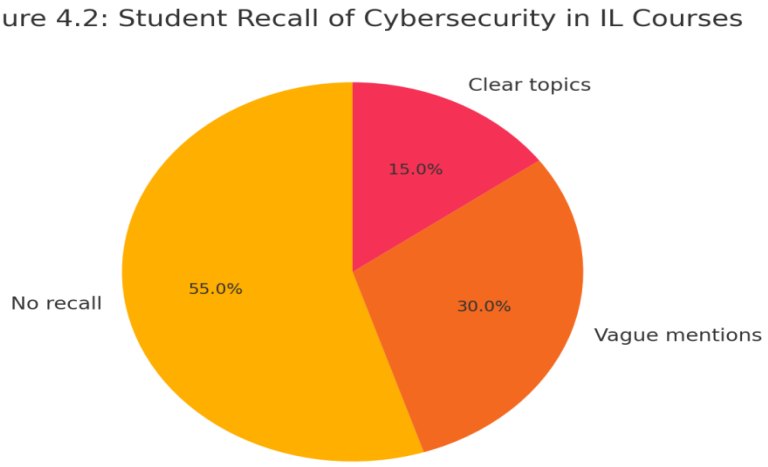

Figure 4: Student Recall of Cybersecurity in IL Courses (Pie Chart)

Self-Reported Practices: Widespread risky practices reported: Password reuse common (over 60%), low confidence identifying sophisticated phishing (only ~35% felt confident), and infrequent privacy setting reviews. Many relied on informal learning (peers, online searches). Perceived Relevance: Students unanimously agreed cybersecurity skills were highly relevant personally and professionally. Expressed frustration at lack of formal guidance.
Suggestions: Desire for hands-on, practical modules integrated early; simulations (e.g., phishing tests); clear, relatable examples relevant to Nigerian context (mobile scams, social media risks).

Figure 5: Students' Suggestion for Improvement

B. Addressing the Research Objectives:

(a). Current State

Confirms a significant gap. Cybersecurity is not systematically integrated into core IL curricula, remaining peripheral or absent. Traditional IL focus persists. Barriers: Validates major barriers, with faculty expertise/time constraints being paramount. Highlights the critical role of institutional will and policy. Student Practices & Awareness: Reveals a concerning disconnect. Lack of formal instruction correlates with

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.16448756

prevalent risky behaviors, despite student recognition of its importance. IL instruction is missing a crucial opportunity.

(b). Interpretation in Context

Nigeria-Specific Challenges: Resource constraints amplify common global barriers. Urgency heightened by the specific cybercrime landscape ("Yahoo Yahoo," mobile fraud). Need for context-specific examples and solutions. Role of Librarians: Librarians/IL instructors are willing but feel unsupported and undertrained. They are a key leverage point but need empowerment. Beyond Compliance: Integration must move beyond checkbox exercises to foster practical, engrained competencies. Link to NDPR compliance for institutions handling student data.

(c). Implications

For Curriculum Development: Urgent need for revised national (NUC) and institutional IL guidelines explicitly mandating cybersecurity competencies. Requires collaborative development involving librarians, IT security, and faculty. For Pedagogy: Need for active, engaging methods (scenarios, simulations, gamification) suited to resource-limited settings. Micro-learning modules feasible. For Faculty Development: Mandatory, ongoing training for librarians/IL instructors on core cybersecurity concepts and teaching strategies. Utilize train-the-trainer models and online resources. For Institutional Leadership: University management must prioritize cybersecurity literacy as a graduate attribute. Provide resources (time, funding, materials), develop supportive policies, and foster collaboration between Library, IT, and Academic Departments. For National Policy: Regulatory bodies (NUC, NBTE) should mandate cybersecurity integration within core undergraduate competencies, including IL. Support resource development.

(d). Proposed Integration Framework

Guiding Principles: Contextual relevance, Phased implementation, Sustainability, Collaboration, Practicality, Alignment with existing IL frameworks (e.g., ACRL). This framework provides a structured approach to integrating information literacy (IL) into institutional curricula, ensuring adaptability across disciplines while maintaining alignment with established standards (e.g., ACRL Framework for Information Literacy).

Core Objectives: Embed IL competencies within disciplinary contexts. Foster collaboration between librarians, faculty, and stakeholders. Ensure scalable, sustainable implementation. Prioritize measurable outcomes and practical application.

(e). Core Cybersecurity Competencies for Nigerian IL: (Adapted from NIST CSF, ISO 27001 basics):

i. Awareness: Common threats (phishing, malware, social engineering), consequences.
ii. Access Security: Strong password creation/management, MFA basics.
iii. Device & Data Protection: Basic device security updates, data backup concepts, encryption awareness.
iv. Privacy Management: Understanding and managing privacy settings (social media, apps), risks of oversharing.
v. Safe Browsing & Communication: Recognizing suspicious links/attachments, secure website indicators (HTTPS), secure Wi-Fi practices.
vi. Critical Evaluation (Security Lens): Assessing credibility with security risks in mind (e.g., scam websites, fake news used for phishing).
vii. Ethical & Responsible Behavior: Understanding cybercrime laws (NDPR, Cybercrimes Act), responsible disclosure.

VOLUME 1, Issue 3, 2025
https://doi.org/10.5281/zenodo.16448756

(f). Phased Implementation Model

Phase 1 (Short-Term: 0-12 months): Awareness & Embedding.
Mandatory faculty training workshops.

i. Integrate 1-2 core topics (e.g., Password Management & Phishing) into existing IL modules using case studies & short demos.
ii. Develop basic resource repository (localized videos, infographics).
iii. Secure management buy-in & designate champions.

Phase 2 (Medium-Term: 1-2 years): Expansion & Consolidation.

i. Integrate all core competencies systematically across IL curriculum levels.
ii. Develop hands-on labs/simulations (e.g., using free platforms).
iii. Create standardized assessments for cybersecurity IL competencies.
iv. Foster formal Library-IT Security collaboration.

Phase 3 (Long-Term: 2+ years): Sustainability & Culture Shift.

i. Regular curriculum review and updates.
ii. Institutionalized faculty development.
iii. Student peer educator programs.
iv. Contribution to national resource repositories. Research on effectiveness.

Overcoming Barriers: Leverage OERs, seek donor support (e.g., cybersecurity firms), advocate for policy change, start small, demonstrate value through pilot assessments.

V. CONCLUSION

This study provides compelling evidence that cybersecurity fundamentals are critically underserved within core information literacy curricula across Nigerian tertiary institutions. A complex interplay of barriers, primarily lack of trained personnel, time constraints, and insufficient institutional prioritization, hinders effective integration. This gap leaves graduates vulnerable in an increasingly hostile digital environment and undermines national efforts towards digital security and economic growth. The proposed phased framework offers a practical roadmap for institutions to begin bridging this gap. Integrating cybersecurity is not merely an enhancement of information literacy; it is fundamental to its core mission of enabling safe, effective, responsible, and ethical information engagement in the 21st century. Addressing this challenge requires concerted action: Librarians need training and support, curriculum developers must mandate integration, university management must prioritize and resource it, and national bodies must provide clear policy direction. By weaving cybersecurity into the very fabric of information literacy instruction, Nigerian tertiary institutions can empower a generation of digitally resilient graduates, contributing significantly to national cybersecurity posture and sustainable development.

VI. REFERENCES

Adebusuyi, A. S. (2022). Cybercrime in Nigeria: Trends, challenges and the role of digital literacy. Journal of Cybersecurity and Privacy, 2(4), 789-805. https://doi.org/10.3390/jcp2040040

Anunobi, C. V., &Emerole, N. (2020). Information literacy programmes in Nigerian university libraries: A review. Library Philosophy and Practice (e-journal), 4345. https://digitalcommons.unl.edu/libphilprac/4345

Association of College & Research Libraries (ACRL). (2015). Framework for information literacy for higher education. http://www.ala.org/acrl/standards/ilframework

https://doi.org/10.5281/zenodo.16448756

Asogwa, B. E., &Ugwu, C. I. (2019). Status of information literacy instruction in Nigerian universities: A survey. Journal of Academic Librarianship, 45(6), 102051. https://doi.org/10.1016/j.acalib.2019.102051

Ayo, C. K., Adebiyi, A. A., &Oluwadare, S. A. (2021). Cybersecurity awareness in Nigerian universities: A student perspective. International Journal of Information Security Science, 10(1), 1-13.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Buchanan, R., Southgate, E., Smith, S. P., Murray, T., & Noble, B. (2020). Post no photos, leave no trace: Children's digital footprint management strategies. Journal of Information Literacy, 14(1), 4–24. https://doi.org/10.11645/14.1.2680

Correa, M. (2020). Cybersecurity is information literacy. College & Research Libraries News, 81(9), 438. https://doi.org/10.5860/crln.81.9.438

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13–21. https://timreview.ca/article/835

Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.

Economic and Financial Crimes Commission (EFCC). (2023). Annual report & consolidated financial statements for the year ended 31st December 2023. [Specific URL if available online, otherwise cite as personal communication or omit if not publicly accessible].

Eze, U. R., Olusola, O. A., &Olusola, A. J. (2018). Cybercrime awareness among students in Nigerian tertiary institutions: A case study. International Journal of Cyber Criminology, 12(1), 228-245. https://doi.org/10.5281/zenodo.1467860

Furnell, S. (2021). The cybersecurity workforce and skills. Computers & Security, 100, 102080. https://doi.org/10.1016/j.cose.2020.102080

Germain, J. M., Koltay, T., &Seadle, M. (2020). Teaching cybersecurity in information literacy instruction: A scoping review. The Journal of Academic Librarianship, 46(5), 102196. https://doi.org/10.1016/j.acalib.2020.102196

Mackey, T. P., & Jacobson, T. E. (2011). Reframing information literacy as a metaliterary. College & Research Libraries, 72(1), 62–78. https://doi.org/10.5860/crl-76r1

Mery, Y., Newby, J., &Peng, K. (2012). Why one-shot information literacy sessions are not the future of instruction: A case for online credit courses. College & Research Libraries, 73(4), 366–377. https://doi.org/10.5860/crl-271

National Information Technology Development Agency (NITDA). (2019). Nigeria Data Protection Regulation (NDPR). https://nitda.gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf

National Universities Commission (NUC). (2021). Benchmark minimum academic standards for undergraduate programmes in Nigerian universities. (Specific edition/year). NUC. [If specific URL unavailable, cite as organization report].

Ojedokun, A. A., &Owolabi, E. O. (2020). Digital literacy skills among undergraduate students of universities in Ogun State, Nigeria. Journal of Library and Information Sciences, 8(1), 1-16. https://doi.org/10.15640/jlis.v8n1a1

Okon, E. O., Udosen, I. E., &Ekpenyong, M. E. (2020). Cybercrime awareness and prevention among university students in Nigeria: A case study. International Journal of Innovative Science and Research Technology, 5(5), 407-414.

Ribble, M. (2015). Digital citizenship in schools: Nine elements all students should know (3rd ed.). International Society for Technology in Education (ISTE).

Webber, S., & Johnston, B. (2017). Information literacy: Conceptions, context and the formation of the citizen. In Information literacy in the workplace (pp. 57-68). Facet Publishing. https://doi.org/10.29085/9781783301344.005