Digital Library Perspective
DOI: 10.1108/DLP-04-2026-0152
Accepted: 24 August 2026
License 4.0 (CC BY-NC 4.0)

Cybersecurity Capacity Building in the Age of Digital Libraries: African Librarians' Perspectives

Nkiruka E. Iwundu[1] and Hussein Suleman[2]
[1]*University of Cape Town & University of Nigeria, Nsukka, Nkiruka.Iwundu@uct.ac.za*
[2]*University of Cape Town, South Africa, Hussein.Suleman@uct.ac.za*

Abstract:

In this era of digital transformation, libraries have evolved from traditional physical repositories of knowledge into dynamic online learning commons. This shift depends on complex, interconnected computer networks that create vulnerabilities and opportunities for cyberattacks. Consequently, libraries have seen a rise in sophisticated cyber threats, raising concerns about data protection, confidentiality, and the integrity of digital content. Strengthening librarians' cybersecurity capacity is essential, as human factors are key to preventing breaches and supporting resilient digital services. This study adapted the National Initiative for Cybersecurity Education (NICE) framework to assess African librarians' cybersecurity proficiency and identify existing skill gaps. The study adopted an exploratory research design. 74 librarians from Ghana, Nigeria, Tanzania, Malawi, South Africa, Uganda, Zambia, Botswana, Zimbabwe, and Kenya participated in the study. Data were collected through a structured questionnaire aligned with the NICE framework and a semi-structured interview. The findings revealed limited awareness and a significant skills gap among librarians. The study also identified five emerging themes: protection of library assets; patrons' data and trust; awareness and skills gaps; cybersecurity education and capacity building; institutional and resource barriers; and an indifferent attitude among staff toward cybersecurity. This article is significant because it offers new insights into improving capacity and strengthening information security. It contributes to knowledge by adapting the knowledge manager and database administrator roles in the NICE framework to assess librarians' cybersecurity skills for digital library services; empirically examining the cybersecurity skill proficiency of African librarians; and identifying critical skill gaps and priority areas for targeted capacity-building and upskilling interventions.

Keywords: *Cybersecurity; skills; capacity building; digital libraries; Africa; data protection*

Introduction

Secured digital library services are widely recognized as essential to the reliability and accessibility of information. By leveraging technology, libraries have extended their traditional operations beyond geographic boundaries, enabling continuous access to resources. According to Jie and Bao-Zhang (2012), the main functions of a digital library include: the collection, storage, and processing of knowledge; providing user-friendly interfaces; offering robust network connectivity; supporting traditional library functions; and enabling efficient retrieval and inquiry services. The services digital libraries provide to patrons are so integral that they are increasingly regarded as part of critical infrastructure systems whose continued operation is vital to societal functioning (CISA, 2024; Hovious & Becker, 2025; Bellini, 2025).

The interconnectedness and inter-reliance of cultural cyber critical ecosystems (Bellini, 2025) underscore the need for cybersecurity as a critical requirement for their protection, resilience, and sustainability. Quintana et al. (2024) defined cybersecurity as the prevention of damage to, protection of, and restoration of computers, electronic communications systems and services, and the information they contain, to ensure availability, integrity, authentication, confidentiality, and non-repudiation. Digital library services operate in an interconnected environment, linking to a broader university network and to many third-party service providers and vendors through vast, interlinked networks. While these connections enable libraries to serve large numbers of patrons across multiple systems, they also expose them to risks, including malware, ransomware, and denial-of-service attacks. Libraries are attractive targets for cyberattacks because of the vast amount of valuable information they hold, including personal data, politically sensitive or governmental information, and research findings. Moreover, libraries often lack full-time system administrators and security specialists and continue to rely on outdated or legacy systems (Corrado, 2024), increasing the risk of data breaches, unauthorized access, and cyberattacks on library systems. As custodians of digital collections, librarians must develop skills to safeguard infrastructure, preserve users' privacy, and maximize the value of library resources by ensuring confidentiality, integrity, and availability through capacity-building programs.

Capacity building is training provided to the workforce to develop specific skills that enhance performance. According to Okwelle and Ebikeseye (2022), capacity building refers to efforts to enhance an individual's knowledge, skills, and attitudes to improve proficiency in a

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

specific task or job. It focuses on strengthening individual abilities to increase efficiency and productivity. In this context, building cybersecurity capacity refers to efforts to enhance librarians' skills to safeguard resources, data, users' personal information, and services in cyberspace. Capacity building and the development of the right skills are essential for librarians, particularly in Africa, where the workforce was reported to be far from its potential (Signe, 2023). Libraries in Africa can only compete and participate in the fourth industrial revolution if their workforce possesses the right skills. This study explored the views of librarians working in academic, public, and special libraries in Africa on this subject. The main purpose of the paper was addressed through the following research questions:

1. What is the librarians' level of awareness of cybersecurity?
2. What is the cybersecurity skill proficiency level of librarians in Africa?
3. What is the level of importance of cybersecurity skills to librarians' job responsibilities?
4. What is the gap in cybersecurity skills among librarians in Africa?

Review of related literature

This section presents cybersecurity skills, Anderson's Adaptive Control of Thought (ACT), and Trist and Bamforth's Socio-technical Theory in relation to the study. It also introduces the National Initiative for Cybersecurity Education (NICE) workforce framework and related works.

Cybersecurity skills

Skill has been defined in various ways and is highly relevant to the effective management of digital libraries. According to Carlton and Levy (2015), skill is a combination of knowledge, experience, and ability that enables effective performance. Bendler and Felderer (2023) emphasized skill as the proficient application of knowledge to meet situational demands securely. Green (2021) highlighted that skills are productive, expandable, and social. They also create value and can be enhanced through training and capacity building. Skills development in cybersecurity for digital libraries could be achieved by training new librarian profiles with cybersecurity skills or by pairing them with sector experts to protect digital assets and ensure service continuity (Bellini, 2024). . Building on the earlier definition of cybersecurity, this study conceptualizes

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

cybersecurity skills as the knowledge and capacity to prevent, protect, and recover systems, networks, and data, ensuring integrity, confidentiality, and availability.

Over the years, librarians and information professionals have seen their skills and roles evolve continuously. The literature has extensively examined these changes (Middleton, 2003; Gerolimos & Konsta, 2008), documenting the shift from traditional core information and knowledge management skills (Gerolimos, 2009) to systems-related skills (Middleton, 2003), contemporary professional skills (Partridge, Menzies, Lee, & Munro, 2010), and digital-era competencies (Raju, 2014). This raises an important question: are these transformations driven by the increasing integration of technology into library services or by the critical value of the resources and data libraries manage? Regardless of the cause, the rapid pace of change underscores the need for continuous reskilling and upskilling among librarians to prevent widening skill gaps. A skills gap exists when there is a disparity between the skills required for a task and those currently possessed by the workforce (Okwelle & Ebikeseye, 2022; Ayodele, Oladokun, & Shakantu, 2020).

Scholars have documented a global shortage of cybersecurity professionals (Vogel, 2016; Deniz, 2022; Blackwood-Brown, Levy, & D'Arcy, 2021; Quintana et al., 2024). In particular, African countries ranked as the least resilient in cybersecurity (Signe, 2023), consistently scoring lowest across all five pillars of the International Telecommunication Union's Global Cybersecurity Index (ITU-GCI): capacity building, legal, technical, organizational, and cooperation. Studies further indicated that African countries are highly vulnerable to cyberattacks due to weak network and information security systems and the widespread use of pirated software (Asongu, 2014), among other factors. Growing concern about the cybersecurity skills gap has led to initiatives such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework, designed to strengthen competencies and bridge the gap (Petersen, 2020). Addressing these gaps requires targeted, intentional capacity-building efforts.

Theoretical framework

Adaptive Control of Thought (ACT) model

The theoretical construct underpinning skills acquisition in this study was drawn from Anderson's Adaptive Control of Thought (ACT) model, which proposed that skills development progresses through three stages: declarative knowledge, procedural knowledge, and

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

automatization (Anderson, 1982). At the declarative stage, information is provided to an individual, who becomes aware of the skill. The transition from declarative to procedural knowledge is crucial for mastering complex skills, such as cybersecurity. In organizations where the security of systems, networks, resources, and sensitive personal data is highly prioritized, workers' capabilities in handling and safeguarding assets move beyond the awareness stage and progress to the procedural stage. This is where they employ techniques and move to the automatization stage, where cybersecurity knowledge, skills, and abilities are executed automatically as routines to mitigate the continuously evolving nature of cyberattacks.

Socio-technical theory

The integration of new technologies, including cybersecurity measures to protect systems, networks, and personal data, often introduces complex processes involving multiple interdependent subsystems. Organizational technological development must therefore account for interactions among these subsystems and how such changes affect the broader work environment. Trist and Bamforth's (1950) study of coal miners, which gave rise to socio-technical theory, demonstrated that changes in mining technology produced significant social effects that, in turn, influenced the effectiveness of the new technology. The central principle of socio-technical theory is joint optimization, which stresses that both the technical and social subsystems of an organization must be optimized simultaneously; otherwise, overall system performance may be compromised.

In the context of cybersecurity, this principle is particularly relevant. Cyber threats are continuously evolving, so organizations must secure not only their technological infrastructure but also the human and organizational subsystems that support it (Aaltola, Ruoslahti, & Heinonen, 2022). According to Paulsen et al. (2012), the distributed and interconnected structure of cyberspace consistently shows that a weakness at one point often significantly affects the security of another. Too often, cybersecurity responsibilities are concentrated within IT or risk management departments, which is insufficient for building robust defenses. As Brill, cited in Petrowicz (2021), observed, effective cybersecurity requires that every organizational unit understand its role in safeguarding data. Thus, successful implementation demands attention to both the technical and social systems, including staff training and the cultivation of a strong security culture.

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Further research highlights the critical role of people in advancing cybersecurity. Colabianchi (2025), Khadka and Ullah (2025), and Abzakh and Althunibat (2023) found that individuals lacking cybersecurity awareness are highly vulnerable to social engineering, phishing, and spoofing attacks. This underscores the need to optimize personnel's knowledge, skills, and abilities through capacity building, supported by continuous training and the acquisition of new competencies (Ruoslahti, 2020). By aligning technical defenses with human capability development, organizations can better withstand evolving threats and ensure the continuity of secure services.

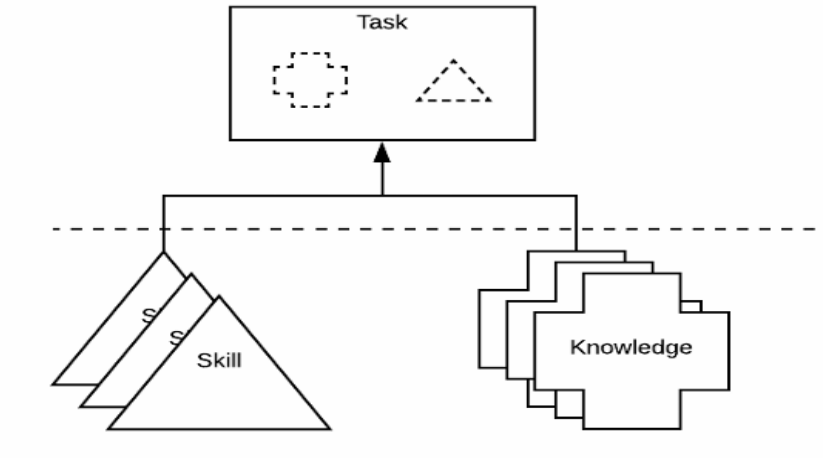
National Initiative for Cybersecurity Education (NICE) workforce framework

Cybersecurity spans a wide range of fields, and the skills required likewise span both technical and non-technical domains. Given this breadth, contributions to cybersecurity come from multiple disciplines, although its foundational roots lie in computer science, information technology, and information systems (Furnell, 2020). Because of this diversity, it is essential to identify the specific skills required for a workforce role. These skills vary in scope, target groups, and assessment methods. Effective skills assessment should be grounded in a recognized skills framework or taxonomy, aligned with appropriate proficiency levels, and directly linked to the actual tasks demanded by the job (Aaltola, Ruoslahti, & Heinonen, 2022; Nevmerzhitskaya et al., 2019). This informed the use of the NICE workforce framework in this study to assess librarians' cybersecurity skill proficiency for effective digital library services. According to Paulsen et al. (2012), NICE seeks to establish an operational, sustainable, and continuously advancing program for cybersecurity awareness, education, training, and workforce development to measurably improve long-term cybersecurity posture. The NICE framework consists of five categories and eleven competency areas, which are broken down into forty-one work roles; each work role has a list of associated knowledge, skills, and tasks.

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Figure 1

NICE Framework Building Blocks Approach



Source: Petersen et al, (2020)

The NICE framework's building block describes a Task as work to be completed. It is defined as an activity directed toward achieving organizational objectives. A Task statement should be straightforward and aligned with the organization's context. Figure 1 illustrates how the Task relates to knowledge and skills. This suggests that to complete a Task, one must possess the knowledge and skills, or challenge oneself to acquire them.

Related works

Aleminda (2025) used a qualitative content analysis combined with comparative analysis to evaluate the key cybersecurity skills emphasized in ten (10) European Union-based cybersecurity frameworks, comparing their structures, scopes, and focus areas and identifying their main strengths and limitations. Quintana et al. (2024) adopted an exploratory design to identify cybersecurity trends affecting criminal justice professionals and to articulate the cybersecurity skills, knowledge, and abilities they need to succeed upon graduation. In a study on fostering cybersecurity in institutional repositories: a case of Nigerian universities, Njoku et al. (2023) reported that a sizable proportion of the librarians they studied believed that cyber threats exist outside the library and that they lacked technical oversight of their domain. Similarly, Fox, cited in Kuzma (2010), explained that the majority of users and librarians are unaware of the security threats to their networks and systems. Muhammad's (2025) study on cybersecurity threats in Pakistani academic libraries in the era of artificial intelligence revealed that, although librarians

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

possess a certain level of awareness, more education is required, and cybersecurity topics should be included in the library training curriculum. In a related study, Aji and Sule (2023) found that library stakeholders are not adequately informed about cybersecurity relevant to the library, which has led to inadequate cybersecurity infrastructure.

Alia (2023) found that the training needs of information specialists at Saudi University included risk assessment, vulnerability management, and the identification and implementation of security controls for managing libraries, among other areas. These needs require training to enhance the skills and competencies of information specialists and keep pace with cybersecurity. Akor et al. (2024) identified artificial intelligence, machine learning, blockchain, and biometric authentication as crucial tools for mitigating cyber threats and as offering transformative capabilities and skills for securing library collections. Bellini and Degl'Innocenti (2025) investigated the foundations of cyber humanities by conceptualizing a cultural cyber-critical ecosystem. Their research examined the evolving relationship among digital transformation, cybersecurity, and cultural heritage management. The study contends that the growing reliance of libraries, archives, and museums on digital infrastructures has transformed these institutions into complex cyber-physical ecosystems, necessitating innovative approaches to preservation, accessibility, governance, and resilience. They present the Cultural Cyber-Critical Ecosystem (C3E) framework, which views digital cultural heritage as an interconnected, interdependent system. The framework positions cultural heritage institutions as both custodians of information resources and critical actors responsible for safeguarding digital assets against emerging cyber threats.

The literature has largely focused on comparative analyses of cybersecurity skill frameworks, the effects of cybersecurity trends on criminal justice professionals, and levels of cybersecurity awareness among information specialists. Despite these advances, librarians' cybersecurity skills in digital library contexts, particularly in Africa, remain underexplored. To address this gap, this study contributes by: (1) adapting the knowledge manager and database administrator roles in the NICE framework to assess librarians' cybersecurity skills for digital library services; (2) empirically examining the cybersecurity skill proficiency of African librarians; and (3) identifying critical skills gaps and priority areas for targeted capacity-building and upskilling interventions.

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Methodology

The study adopted an exploratory research design. Exploratory research is conducted in new or emerging areas (Jha, 2023; Haile, 2023; Rahmon, Osademe, Ononokpono, 2023). An exploratory design was appropriate because, to the best of the researchers' knowledge, little or no research has been conducted on building cybersecurity capacity for digital library services in Africa. The study population comprised librarians associated with all digital libraries/repositories in Africa. The study employed convenience sampling to select respondents.

The instrument for data collection in the study adopted the NICE Framework Components Version 2.0.0 as the foundational reference for identifying relevant cybersecurity knowledge and skills applicable to library professionals. The NICE Framework Components are supported by a spreadsheet reference document developed to facilitate the use and application of the framework. This document is available at (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions). It provides a structured description of cybersecurity workforce components, including categories, work roles, work role descriptions, work role identifiers, associated knowledge areas, skills, and tasks required for each work role.

For this study, the Knowledge Manager and Database Manager roles were selected for their conceptual alignment with librarians' professional responsibilities. All skills associated with these roles were incorporated, and knowledge areas specific to knowledge management responsibilities were identified and adapted to reflect the terminology and professional context of library and information science. This adaptation ensured that the cybersecurity skills were appropriately contextualized to the roles, practices, and responsibilities of library professionals. In total, 33 relevant skills were identified and incorporated into the study's instrument (survey). The instrument was validated by two experts in computer science and library and information science. In addition, the instrument received approval from the ethics committee for data collection.

At the data collection stage, an online survey (https://limesurvey.uct.ac.za/index.php/799161?lang=en) was administered to assess librarians' proficiency in cybersecurity skills. Participants were recruited through library conferences attended by the researchers, professional network platforms, and contact information obtained from staff directories on library websites. A total of 110 invitations (sent via email and WhatsApp) containing the survey link were distributed, and 74 (67%) complete responses were found useful

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

for the study after data cleaning. After analyzing the data using descriptive statistics, a smaller sample of respondents who indicated willingness to participate in the second-stage data collection through a semi-structured interview (see appendices) was interviewed to gain in-depth insight into the findings and their personal experiences. Data collected during the interview (audio recordings) were transcribed in Microsoft Word. Thematic analysis was used to code and identify themes within the interview data.

Ethical approval was granted by the University of Cape Town Faculty of Science Research Ethics Committee (No. SCI/02054/2025) on 25 August, 2025. Participants were fully informed about the purpose of the research, participation was voluntary, and their identities and data were protected.

Results

Seventy-four (74) willing participants from Ghana, Nigeria, Tanzania, Malawi, South Africa, Uganda, Botswana, Zambia, Zimbabwe, and Kenya completed the survey, and seven (7) librarians participated in the interview. Early findings from this work, drawn from the literature and initial survey data, were presented as a conference paper at the Standing Conference of Eastern, Central, and Southern Africa Library and Information Association. This paper presents findings, additional survey data, and interview results.

Demographic Factors of the Participants

Figure 2 presents the demographic characteristics of the seventy-four (74) librarians who responded to the survey. Years of work experience vary among participants, with the largest proportion, 24 (32%), having 6–10 years of experience. In terms of rank, assistant librarians constitute the largest share of respondents, 21 (28%), followed by senior librarians, 20 (27%). Most participants are librarians from academic libraries, 58 (78.4%), public libraries, 12 (16.2%), and special libraries, 4 (5.4%). Notably, 35% and 33% of the participants are from Malawi and Nigeria, respectively, whereas 3% each are from Ghana, Botswana, and Uganda. The variation is a result of librarians' unwillingness to participate in the study across many countries, even after many reminders.

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

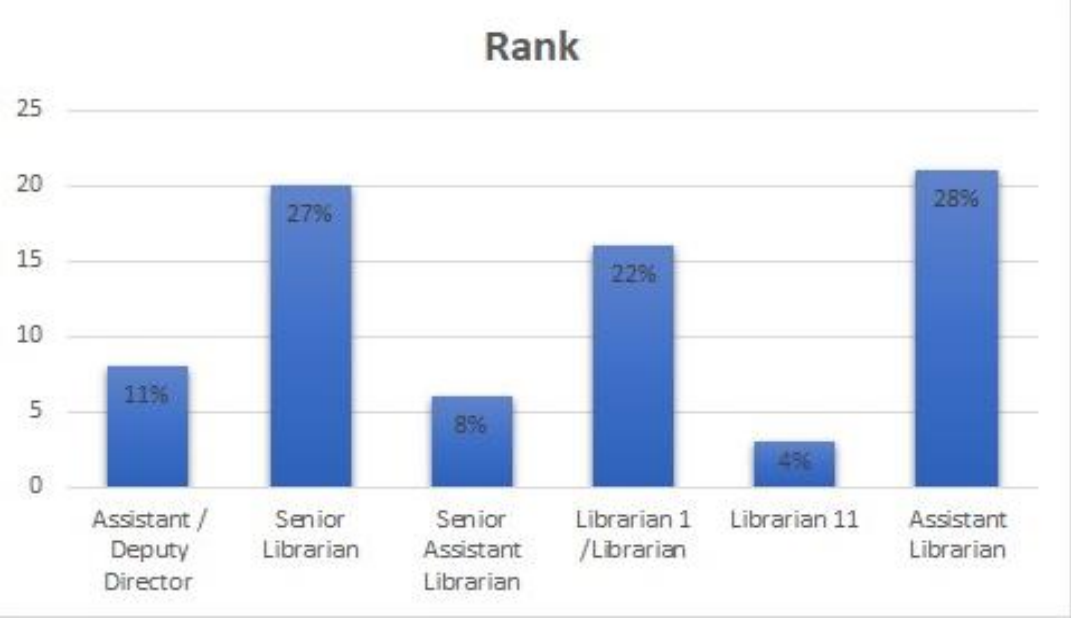
Demographic Factors of the Participants

Figure 2.1 Years of Work Experience



Source: Field Survey

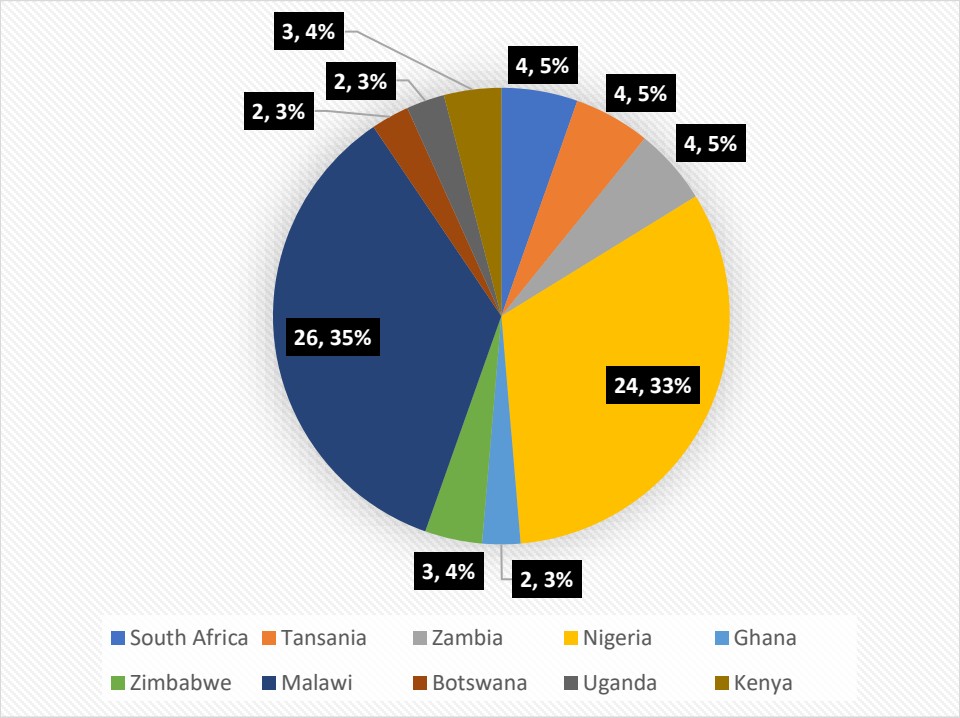
Figure 2.2 Professional Rank



Source: Field Survey

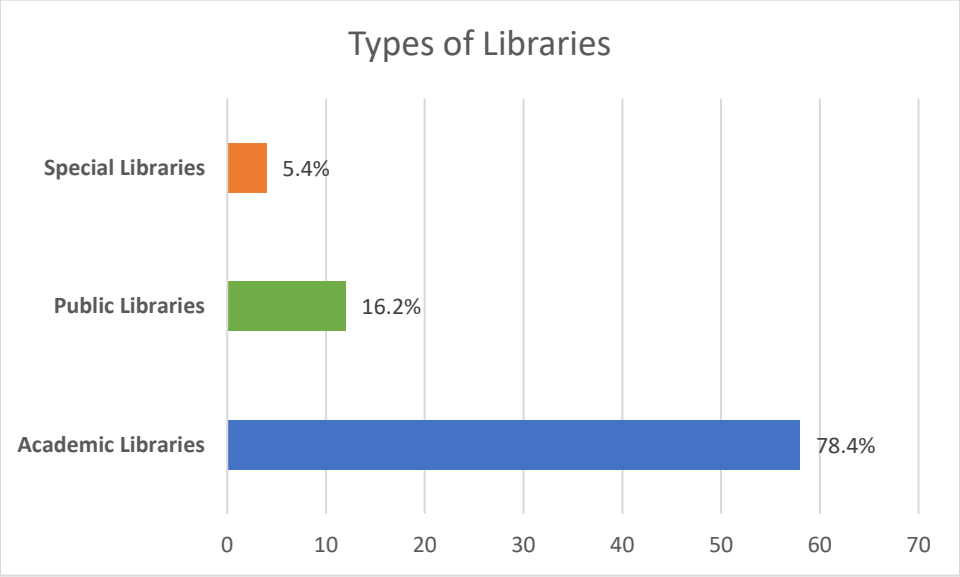
DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Figure 2.3 Country of Origin



Source: Field Survey

Figure 2.4 Types of Libraries



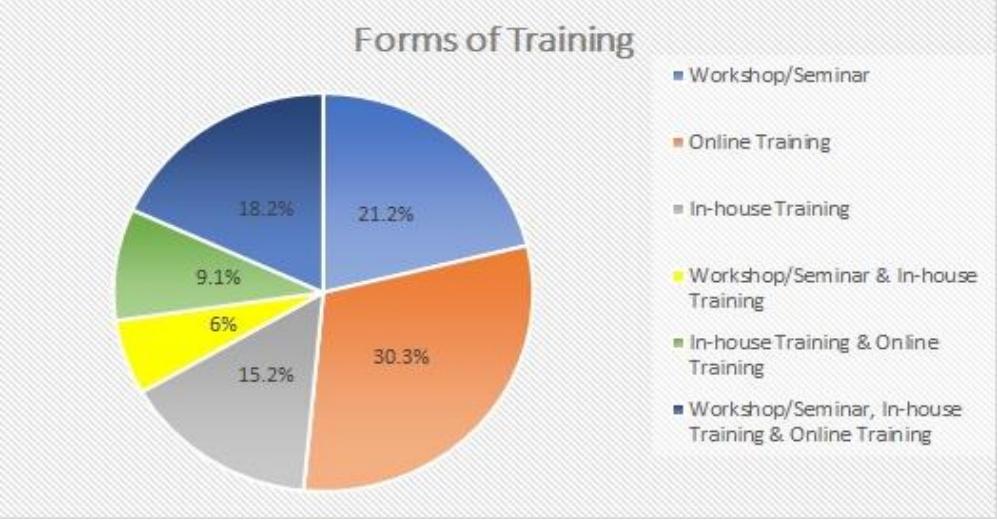
Source: Field Survey

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Research Question 1: “What is the librarian's level of awareness of cybersecurity?”

The findings revealed that 41 (55%) of the librarians reported being unaware of and not having received any training on data protection and the security of digital library resources. In contrast, 33 (45%) indicated that they are aware and have been trained in protecting data and digital library resources.

Figure 3 Training Methods



Source: Field Survey

Of the 33 (45%) respondents who reported being aware and having received training, 30.3% received training via online platforms, 21.2% through workshops and seminars, and 15.2% through in-house training (Figure 3). While all training methods can be effective, particular emphasis should be placed on approaches that promote hands-on, practical exercises, as these foster deeper engagement and skill mastery.

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Figure 4. Level of Skills Proficiency of Librarians



Source: Field Survey

A total of thirty-three (33) skills identified from the NICE framework of knowledge and database managers' skill sets were grouped into three categories: information and knowledge management; digital information management; cybersecurity, data protection, and governance.

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

To answer Research Question 2, “What is the cybersecurity skill proficiency level of librarians in Africa?” librarians were presented with a list of these specific skills and asked to rate their proficiency on a scale of 1 to 5, where 1 indicated no proficiency and 5 indicated expert proficiency. The results are presented in Figure 4. Notably, information and knowledge management skills achieved the highest mean ratings. For example, the skill “cataloguing and classification of information” ranked highest, with a mean score of 3.61 (see Figure 4). In contrast, “plan and manage the delivery of knowledge management project” ranked lowest within this category, with a mean score of 2.78. Overall, these scores generally fall within the intermediate (2.61–3.40) to advanced proficiency (3.41–4.20) ranges, which is unsurprising given that these are foundational skills cultivated through LIS education and practice.

Most digital information management skill categories are rated at intermediate proficiency, with mean scores ranging from 2.72 to 3.03. A notable exception in this group is “inspecting and preparing data for ingestion,” which has a lower mean score of 2.55. Cybersecurity, data protection, and governance skills have the lowest ratings, with mean scores from 2.03 to 2.64, placing them in the basic proficiency range (1.81–2.60). However, within these lowest-rated categories, “using tools that protect personal data when cleaning or archiving digital content” (2.89) and “developing policy plans” (2.77) are exceptions, as their scores fall within the intermediate range.

To answer Research Question 3, "What is the level of importance of cybersecurity skills to librarians' job responsibilities? Participants rated each skill's importance to their duties on a scale from 1 (not important) to 5 (extremely important). Figure 5 presents the results. “cataloging and classification of information” had the highest mean score, 4.14, while “preparing reports on user engagement and access patterns” had the lowest, 3.68. All scores fall within the "very important" range (3.41–4.20) (see Figure 5), suggesting these skills are crucial for librarians. A gap analysis (see Figure 6) identified the most critical training areas by calculating the mean difference between the importance and proficiency levels for each skill. The study adapted Ayodele, Oladokun, and Shakantu's (2020) hypothetical scale to categorize the skill gap for each skill as follows:

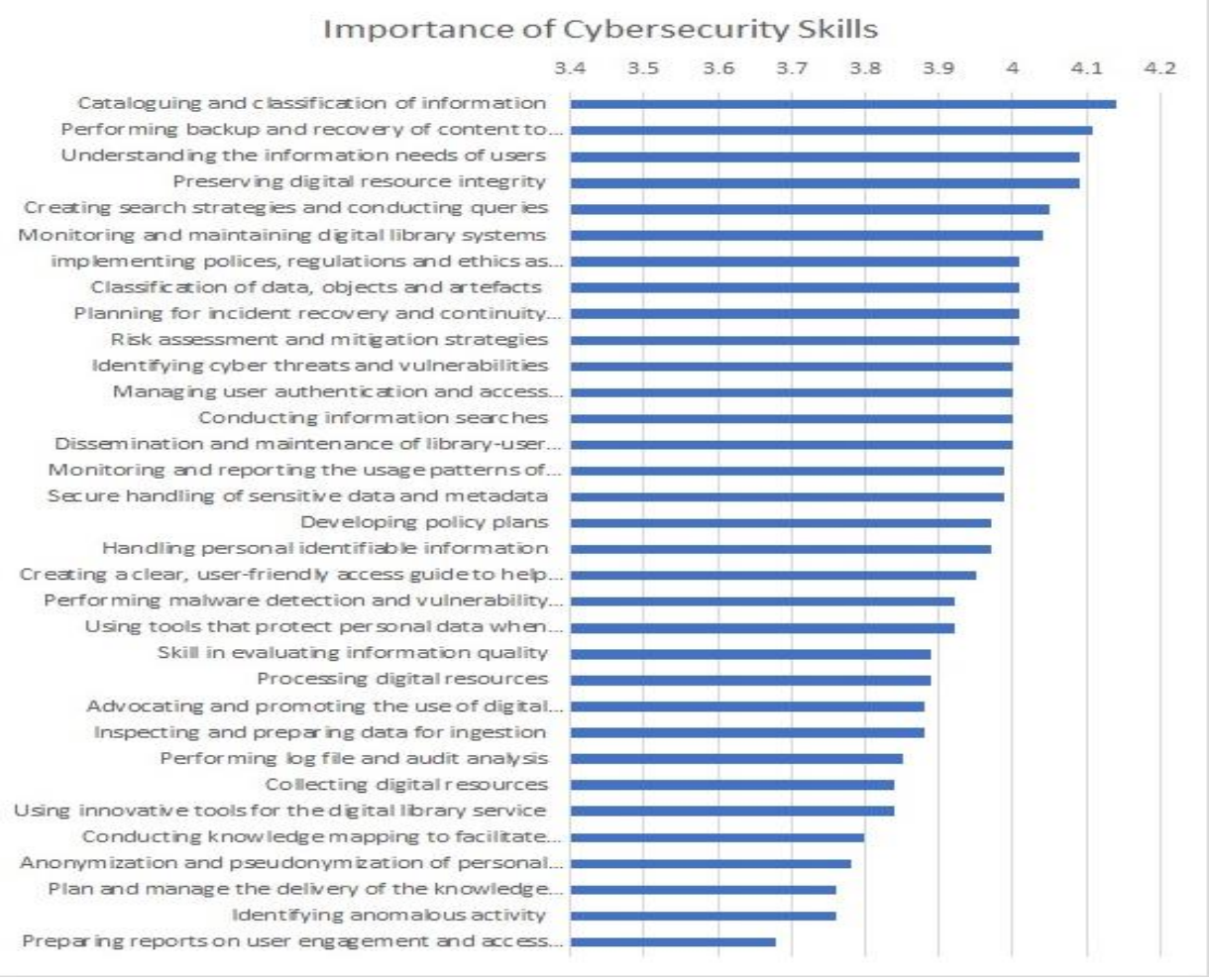
- mean value greater than 1.50 – very high priority;
- mean value from 1.00 to 1.49 – high priority;
- mean value from 0.50 to 0.99 – moderate priority;

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

- mean value from 0.01 to 0.49 – low priority; and
- mean value less than 0.01 – no skill gap.

Performing log file and audit analysis (1.82), performing malware detection and vulnerability scans (1.76), and identifying cyber threats and vulnerabilities (1.69) are the top training priorities (see Figure 6). Additional priorities include planning for incident recovery and continuity (1.67), implementing policies, regulations, and ethics related to cybersecurity and privacy (1.63), and handling personal identifiable information (1.51). Skill gaps above 1.50 are considered very high priority and encompass most cybersecurity, data protection, and governance skills. This points to a significant cybersecurity skills gap among librarians in Africa.

Figure 5. Level of Importance of Cybersecurity Skills on Job Responsibilities



Source: Field Survey

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Figure 6. Gap Analysis



Source: Field Survey

Emerging Themes on Cybersecurity Skills, Trends, and Challenges in African Libraries

Thematic analysis of interview data from seven participants (P1, P2, P3, P4, P5, P6, P7) was conducted in Microsoft Excel. Approximately 65 small segments of information were extracted

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

from the transcripts and entered into a Microsoft Excel spreadsheet for initial coding, guided by the research questions. The initial codes underwent iterative review and refinement in a second coding cycle to improve clarity and reveal underlying patterns. Related codes were grouped into 27 categories based on conceptual similarities. These categories were subsequently examined, counted, and consolidated into the following five themes (see Table 1. Appendix).

- Protection of Library Assets, Patrons' Data, and Trust
- Awareness and Skill Gap
- Cybersecurity Education and Capacity Building
- Institutional and Resource Barriers
- Indifferent Attitude of Staff toward Cybersecurity

Protection of Library Assets, Patrons' Data, and Trust

The findings highlighted consistent emphasis among librarians on protecting library assets and on concerns about real-world incidents and cyber threats. Respondents emphasized that cybersecurity is critical for protecting digital library systems and personal data and for sustaining users' confidence. They opined that breaches have reputational consequences and could erode the trust of researchers who archived their data and use digital libraries. In addition, mentions of attacks indicate that cyber threats are not merely theoretical but are already occurring, calling for proactive measures.

"*Cybersecurity is critical to our electronic libraries because a breach in any of our subscribed databases can compromise the entire organization*" –[P1].

He further stated that "*lack of proper measures to protect data in the repository could undermine trust among content submitters (researchers). Without confidence that their sensitive data will be adequately safeguarded, researchers may hesitate to share information, especially if they perceive risks of poor repository management*" –[P1]. "*Patrons can trust the information in our custody because that information is protected" –* [P4].

Another participant affirmed that:

"Cybersecurity is very important to us in national and cultural heritage libraries, as there is historical and politically sensitive information about the nation that hackers fighting the nation in cyber war are interested in. There are occasions when……. alarms about hackers trying to breach our systems were raised not just once or twice, but several times, with several unauthorized persons trying to log in to our servers" –[P2].

A participant narrated incidents that occurred in their libraries:

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

"Cybersecurity is critical in digital libraries because we have had two incidents that we are yet to recover from. Our library experienced the loss of all cataloging metadata and the indexed card entries saved on the server due to malware. There was a similar case when the library lost 21,000 digitized theses and dissertations from the then-repository. Those incidents caused a major setback and a huge loss because, in the case of the repository, a lot of money had been invested in the project, and massive equipment had been purchased, including servers and a high-capacity generator. Casual workers were hired and trained to digitize the theses and dissertations, but since then, populating the repository with that many records have not been done" –[P3].

"Cybersecurity is necessary because attempts to recover data after an incident are always partial, and most of the recovered files may be corrupted" –[P5].

Awareness and Skill Gap

As previously discussed, the information profession is changing rapidly due to technological developments. The roles and responsibilities of librarians are evolving, and staying relevant requires continuous awareness, upskilling, and reskilling. Participants in this study noted that this dynamic shift has created a skills gap and that librarians increasingly rely on a small number of IT personnel within their institutions to perform core cybersecurity tasks, thereby jeopardizing library assets and the profession. One participant highlighted that "Librarians are the custodians of valuable data; hence, they need to acquire skills in data management, preservation, and protection. In particular, they need skills in access control, the ability to prevent unauthorized actions in their systems, and the ability to perform basic system upgrades and back-up tasks" –[P2].

Another participant reported that "Librarians should have data management skills, such as de-identification of research data, basic technical skills such as routine data backup, vulnerability scanning, and software upgrades, and managerial and governance skills to manage and oversee library assets. They should also develop effective communication and conceptual skills to report malicious or suspicious activities" –[P4].

A participant mentioned, "the challenge of low speed in awareness creation. The pace at which awareness and sensitization programs are implemented is not encouraging, given the increase in cyber incidents. Organizations should move quickly, create weekly sensitization or awareness materials, and not wait until an incident occurs" –[P5]. "Training in cybersecurity was not frequent as it ought to be……this should be quarterly if not continuous" –[P6].

However, another participant indicated, "I do not expect library staff, in the sense of information professionals, to have core cybersecurity technical skills…… these technical skills come at a price tag and are sought after……. the skills lie mainly with system administrators and not information professionals" –[P7].

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Cybersecurity Education and Capacity Building

Another common theme that emerged from the findings was the need for structured training and continuous professional development focused on the security of digital library assets. The findings also revealed the need to integrate cybersecurity courses into the library and information science curricula to help students develop employability skills. Some participants reported having no formal training on the subject, while others acknowledged that awareness and training programs had been implemented in their institutions; however, these initiatives are not comprehensive enough to build meaningful cybersecurity capacity. There was consensus among the participants that education and capacity building are core pillars of cybersecurity success in any organization, as cybersecurity is not just for technical experts but for all professionals, helping to develop a culture of cyber hygiene. For instance, the participants said:

"We lack understanding of how a cyberattack could affect our organization or how it might occur. We need training on these risks. Incorporating cybersecurity courses from the undergraduate to the postgraduate levels will build awareness and essential skills among librarians" -[P1].

"*We had a management-level sensitization program on data protection and digital collection, during which I learned about cybersecurity. I can say that there is not enough capacity-building in this field of cybersecurity yet*" –[P2].

The findings also showed that cybersecurity training is an institutional responsibility. "*Training on cybersecurity is an institutional concern, is not done specifically by the library…….neither has the library promoted cybersecurity training from its own end"* –[P5]. Additionally, an interviewee reported that: *"In my institution, there was university cybersecurity training. But few people were selected for that training; I am not sure anyone from the library was selected. There appears to be an assumption that the library is not a high-risk setting"* –[P3].

Institutional and Resource Barriers

Across participants, several factors emerged as significant barriers to acquiring cybersecurity skills. The most common were organizational priorities and funding constraints, which were identified as major obstacles to implementing cybersecurity training and programs. Organizational priorities are strategic areas that guide institutional planning, resource allocation, and operational decisions, determining which initiatives receive sustained attention and investment. Although cybersecurity is officially recognized as a strategic concern at the institutional level, this study found that leadership often views the library as a low-risk

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

environment within the broader cybersecurity landscape. The findings revealed that librarians view library assets as worthy of prioritization in a cybersecurity plan, whereas some institutional leaders felt that the library did not require such intervention. This perception has limited proactive risk mitigation efforts and weakened the development of operational cyber resilience within the library. Consequently, insufficient funding has been allocated to library-specific cybersecurity initiatives, including staff training and ongoing professional development. The issue of inadequate awareness and training may stem from funding constraints and a shortage of experts and resource persons, as most participants reported that the cost of hiring specialists and organizing training is very high. Another issue raised was the absence of policies governing cybersecurity interventions and awareness. For instance, participants mentioned:

"*Could you imagine that our repository server runs on local servers without adequate measures to safeguard it, then they feel that services on the cloud with mirror servers as backups are more important"*-[P6].

"The last cybersecurity training conducted, nobody was selected from the library to attend" –[P3].

"*Limited funding and resources, experts that will do the training are major barriers, since these trainings cannot be conducted without these factors*" –[P4].

"*Where no formal policies exist to support cybersecurity awareness and training, successful implementation becomes challenging"* –[P6].

Indifferent Attitude of Staff toward Cybersecurity

The findings reveal an indifferent attitude among staff, which significantly constrains the institutions' cybersecurity capacity. Librarians' reliance on systems administrators for cybersecurity functions limits corporate effort, which is essential for effective cyber resilience. In addition, some staff perceived cybersecurity training as irrelevant because it wasn't their core responsibility and was often overshadowed by routine library tasks. These attitudes among librarians suggest that, although they hold positive views of cybersecurity training, their intention to participate is shaped by competing responsibilities and perceived priorities within their roles. To this end, participants (P4, P5 and P7) reported that:

"*Cybersecurity skills are for systems administrators; librarians don't need cybersecurity training. It is for the IT department, and it is not a priority for librarians."* –[P7].

"Balancing time between professional responsibilities and training participation remains a challenge due to conflicting priorities" –[P4].

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

"Cybersecurity training is not mandatory for staff, and I don't think it is library specific" –[P5].

Discussion of Findings

Our exploratory study investigated cybersecurity capacity building in the age of digital libraries. We employed an online survey and interviews to gather data from participants. Overall, the study revealed key emerging themes: protection of library assets, patrons' data, and trust; awareness and skills gaps; cybersecurity education and capacity building; institutional and resource barriers; and an indifferent attitude among staff toward cybersecurity. The study underscored the significance of cybersecurity in the digital age, showing that it not only protects library assets but also builds trust among users. Our findings showed that librarians are unaware of cybersecurity and have not received training on securing digital library resources and protecting data. These findings align with Kuzma (2010) and Njoku et al. (2023), who asserted that librarians are unaware of the security issues affecting their systems and networks and that cyber threats exist outside libraries. Conversely, Muhammad (2025) and Aji and Sule (2023) noted that although librarians have some awareness, they are not adequately informed, and additional cybersecurity training remains necessary.

Additionally, the survey revealed that the majority of those who were aware had online training and were not afforded the opportunity to participate in practical exercises or hands-on sessions. Mastery entails deeper engagement through practice and is essential because it enables employees to perform cybersecurity tasks automatically, as Anderson (1982) described. Workers' capabilities in handling and safeguarding assets should progress from awareness (declarative stage) to the mastery stage (procedural knowledge and automatization). This progression highlights the need to strengthen cybersecurity awareness and sensitization initiatives among library professionals by moving beyond knowledge acquisition toward practical, hands-on training and the integration of cybersecurity practices into everyday library routines and professional responsibilities. Through such continuous practice and application, librarians can develop the competence to execute cybersecurity tasks effectively and consistently, thereby building cyber resilience against potential cyber threats.

The results further revealed that librarians generally demonstrate basic proficiency in cybersecurity and data protection, indicating a largely foundational understanding of these increasingly vital competencies. With such introductory skill levels, librarians may struggle to

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

detect complex cyber threats, leaving libraries vulnerable to cyberattacks, data breaches, and mishandling of sensitive information. This could undermine the trust of researchers, academics, and other library users who rely on the secure management of digital assets. Cybersecurity extends beyond technical measures; therefore, organizations should employ the principle of joint optimization (Trist & Bamforth, 1950), developing and strengthening both the technical and social subsystems simultaneously.

Moreover, the findings revealed a skills gap in cybersecurity skills among librarians in Africa. Prioritizing the development of these abilities should take precedence over other strategic investments. The findings are consistent with those of Vogel (2016), Deniz (2022), Blackwood-Brown, Levy, and D'Arcy (2021), and Quintana et al. (2024), who highlighted the global cybersecurity skill gap. The need to address these priority areas through continuous training cannot be overstated, including implementing a cybersecurity policy, adhering to regulations, and establishing an incident recovery plan. Librarians should have skills in log file and audit analysis because this knowledge will not only reveal threats but also enable monitoring of user access, information resource usage patterns, and preferences, thereby informing library collection development and helping save costs within a stringent budget. Moreover, some libraries still use legacy systems with unpatched vulnerabilities; vulnerability assessments and scanning will reveal the need for upgrades and software patches, moving libraries from reactive responses to proactive protection of their information assets. As libraries embrace new digital technologies to deliver services, there must be accompanying changes in the security landscape and a need to develop new skills to maintain uninterrupted service delivery.

Implications of the findings

Cybersecurity capacity building is critical for all organizations. Administrators should understand that all departments are targets; a compromise in one area is likely to affect others. Intervention strategies should be applied equally across training, infrastructure, and funding.

Awareness is foundational to cybersecurity readiness. Information professionals must understand emerging digital threats, including phishing, ransomware, data breaches, and identity theft, and how they can affect library systems and users' information. Awareness programs will

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

help them recognize risky behaviors, clarify their responsibilities for protecting digital assets, and cultivate a security-conscious mindset.

Capacity-building and training initiatives help workers bridge identified skill gaps, especially in areas such as data protection, access control, vulnerability and audit log assessment, and incident response. Workers should cultivate positive attitudes towards acquiring emerging skills that enhance their expertise and ensure they remain relevant in their profession.

Limitations and further research

Although the findings indicate that librarians possess only basic proficiency in cybersecurity and data protection, there are some limitations: first, the study relies on self-reported data, which may not accurately reflect their skill levels in real-world cybersecurity tasks. The study focused on librarians from a few African nations (Ghana, Nigeria, Tanzania, Malawi, South Africa, Uganda, Zambia, Zimbabwe, and Kenya) who were willing to participate, which may limit the generalizability of the results to libraries in countries with different levels of digital maturity. Consequently, we suggest that further research consider approaches such as direct skills assessments.

Conclusion

Strengthening cybersecurity in digital libraries requires capacity building. Awareness and sensitization initiatives ensure that the workforce understands emerging threats and adopts a proactive security mindset. Training and capacity-building programs address critical skill gaps, equipping staff with the competencies needed to manage digital systems securely. Together, these elements enhance the overall cybersecurity posture of digital libraries, enabling the workforce to protect sensitive data, ensure the integrity of digital services, and support resilient, trustworthy library operations in an increasingly complex digital environment. Cybersecurity is not only about technical measures such as firewalls, cryptography, or AI, but also about people. In Africa, the workforce must evolve as quickly as adversaries, armed with skills and capabilities, because this is our greatest defense.

Acknowledgements

This work is financially supported by the Telkom Centre of Excellence and the University of Cape Town, South Africa.

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

References.

Aaltola, K., Ruoslahti, H. and Heinonem, J. (2022), "Desired cybersecurity skills and skills acquisition methods in the organizations", paper presented at the 21st European Conference on Cyber Warfare and Security, 16-17 June,2022. DOI: https://doi.org/10.34190/eccws.21.1.293

Abzakh, A. and Althunibat, A. (2023), "A review: human factor and cybersecurity", paper presented at the International Conference on Information Technology (ICIT), 9-10 August 2023, Amman, Jordan, 589-592,Doi:10.1109/ICIT58056.2023.10225828.

Aji, K. O. and Sule, Y. (2023), "Curbing security threats in academic libraries: a survey of academic librarians' perception on cybercrime and cybersecurity information in three selected colleges of education in Nigeria". *Information Technology and Librarianship*, Vol. 3 No. 1.

Akor, S. O., Nongo, C., Udofot, C. and Oladokun. B. D. (2024), "Cybersecurity awareness: leveraging emerging technologies in the security and management of Libraries in Higher Education Institutions", *Southern African Journal,* Vol. 2 (July). https://doi.org/10.25159/3005-4222/16671

Aleminda, F., (2025), "Comparative analysis of EU-based cybersecurity skills frameworks", *Computers and Security*, Vol. 151 (2025) 104329

Alia, M. A., (2023), "Training needs of information specialists at Saudi Universities' libraries to achieve cybersecurity requirements", *International Journal of Education and Information Technologies*, Vol. 7, pp.38-50. DOI: 10.46300/9109.2023.17.5

Anderson, J. R. (1982), "Acquisition of cognitive skills", *Psychological Review*, Vol. 89, No.4, pp.369-406.

Asongu, S. (2014), "Software piracy, inequality, and the poor: Evidence from Africa", *Journal of Economic Studies,* Vol. 41, No. 4, pp.526-553. Doi: 10.1108/JES-10-2012-0141

Bendler, D. and Felderer, M. (2023), "Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model", *ACM Trans. Computer Education,* Vol. 23 No.2, pp.1-33. https://doi.org/10.1145/3573205

Bellini, E. (2025). "Cyber Humanities for Heritage Security". *Communications of the ACM*, Vol. 68 No. 12) (December 2025), 112–117. DOI:10.1145/3735659

Bellini, E. and Degl'Innocenti, E. (2025). "Building the Foundations of Cyber Humanities: Cultural Cyber-Critical Ecosystem Conceptualization". 2025 IEEE International Conference on Cyber Humanities (IEEE-CH), Florence, Italy, 2025, pp. 1-8. Doi: 10.1109/IEEE-CH65308.2025.11279317 (accessed 11June 2026).

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

Carlene, B., Yair, L. and John, D. (2021), "Cybersecurity awareness and skills of senior citizens: A motivation perspective, *Journal of Computer Information Systems*, Vol. 61 No.3, pp.195-206, DOI: 10.1080/08874417.2019.1579076

Cybersecurity and Infrastructure Security Agency, (2021). "*What is Cybersecurity?",* available at: https://www.cisa.gov/news-events/news/what-cybersecurity (accessed 15 January, 2026)

Colabianchi, S., Costantino, F., Nonino, F., and Palombi, G. (2025), "Transforming threats into opportunities: The role of human factors in enhancing cybersecurity" *Journal of Innovation and Knowledge,* Vol. 10, 100695. https://doi.org/10.1016/j.jik.2025.100695

Carlton, M. and Levy, Y. (2015), "Expert assessment of the top platform-independent cybersecurity skills for non-IT professionals", paper presented at the IEEE Southeast Conference,9-12 April, 2015, Fort Lauderdale, Florida. **DOI:** 10.1109/SECON.2015.7132932

Deniz, A. (2022), "Analysis of Software Engineering Skills Gap in the Industry", *ACM Trans. Computer. Education.* Vol. 23 No.1, pp.1-28. https://doi.org/10.1145/3567837

Furnell, S. (2020), "The Cybersecurity workforce and skills", *Computer and Security,* Vol.100, 102080

Gerolimos, M. (2009), "Skills developed through library and information science education", *Library Review,* Vol. 58 No.7, pp.527-540. DOI 10.1108/00242530910978217

Green, F. (2021), "What is Skill?", *An inter-disciplinary synthesis*, available at https://www.llakes.ac.uk/publication/what-is-skill-an-inter-disciplinary-synthesis/ (accessed on 23 November, 2025)

Hovious, A. S., and Becker, J. A. (2025), "The Critical infrastructure roles of small and rural Public Libraries", *Public Library Quarterly*, 1–20. https://doi.org/10.1080/01616846.2025.2496169

Jie, S., and Bao-Zhong, Y. (2012), "Development and characteristics of digital library as a library branch". *IERI Procedia,* Vol. 2, pp.12 – 17. https://doi.org/10.1016/j.ieri.2012.06.044

Khadka, K. and Ullah, A. B. (2025), "Human factors in cybersecurity: an interdisciplinary review and framework proposal", *International Journal of Information Security,* Vol. 24 No.119. https://doi.org/10.1007/s10207-025-01032-0

Kuzma, J. (2010), "European digital libraries' web security vulnerabilities", *Library Hi Tech*, Vol. 28 No.3, pp.402-413. DOI 10.1108/07378831011076657

Middleton, M. (2003), "Skills expectations of library graduates", *New Library World,* Vol.104 NO. 1184/1185, pp.42-56. DOI 10.1108/03074800310458278

Muhammad, Y. A. (2025), "Cybersecurity threats in Pakistani academic libraries in the era of artificial

 License 4.0 (CC BY-NC 4.0)

Intelligence", *International Information and Library Review*, Vol.57 No. 2, pp.204-210. https://doi.org/10.1080/10572317.2025.2479289

Njoku, I. S., Njoku, B. C., Chukwu, S. A. J. and Ravichandran, R. (2023), "Fostering cybersecurity in institutional repositories: A case of Nigerian Universities", *African Journal Library Archives and Information Science,* Vol. 33 No. 1, pp.1-21

Partridge, H., Menzies, V., Lee, J, and Munro, C. (2010), "The contemporary librarian: Skills, knowledge, and attributes required in a world of emerging technologies", *Library & Information Science Research,* Vol.32, pp.265–271

Paulsen, C., McDuffie, E., Newhouse, W. and Toth, P. (2012), "NICE: creating a cybersecurity workforce and aware public", *IEEE Security and Privacy*, Vol.10 No. 3, pp76-79. DOI: 10.1109/MSP.2012.73.

Petersen, R., Santos, D., Wetzel, K. A., Smith, M. C., and Witte, G. (2020), "Workforce framework for cybersecurity (NICE Framework)", *NIST Special Publication 800-181 Revision 1*. https://doi.org/10.6028/NIST.SP.800-181r1

Petrowicz, D. (2021). "How libraries can protect themselves from cyberattacks", available at https://www.springernature.com/gp/librarians/the-link/blog/blogposts-news-initiatives/how-libraries-can-protect-themselves-from-cyberattacks /19556496 (accessed on 23 November, 2025)

Quintana, K., Sutton, C. C., Olson, D., and Kosloski, A. (2024), "Cybersecurity skills, knowledge, and abilities for criminal Justice Professionals: An exploratory study of practitioners' perspectives", *Journal of Cybersecurity Education, Research, and Practice*, Vol. 1. DOI: doi.org/10.62915/2472-2707.1175

Ruoslahti, H. (2020), "Business continuity for critical infrastructure operators", *Annals of Disaster Risk Sciences*: ADRS, Vol. 3 No. 1. https://doi.org/10.51381/adrs.v3i1.46

Ruoslahti, H., Coburn, J., Trent, A. and Tikanmäki, I. (2021), "Cyber skills gap - a systematic literature review of academic literature", *Connections: The Quarterly Journal* Vol. 20, pp.33–45 https://doi.org/10.11610/Connections.20.2.04.

Signe, L. (2023), *Africa's Fourth Industrial Revolution*. Cambridge University Press. https://doi.org/10.1017/9781009200004

Tenison, C., and Anderson, J. R. (2016), "Modeling the distinct phases of skill acquisition", *Journal of Experimental Psychology: Learning, Memory, and Cognition,* Vol. 42 No. 5, pp.749-767.

Trist, E., and Bamforth, K. (1951), "Some social and psychological consequences of the longwall method of coal-getting", *Human Relations*, Vol. 4, pp.3–38. DOI: 10.1177/001872675100400101

Vogel R. (2016), "Closing the cybersecurity skills Gap", *Salus Journal,* Vol. 4 No. 2, pp.32-46.

Appendix

Table 1. Overview of the key themes, categories and codes.

Themes	Categories	Second Round of Coding	Initial Coding
Protection of Library Assets, Patrons' Data, and Trust	Organizational assets concern	Database breach risk Critical information assets	A breach in subscribed databases can compromise the organization.
	Data privacy and user trust	Patron data exposure Loss of user trust	Subscribed databases are critical organizational resources.
	Protection of Sensitive Information Assets	Loss of contributor trust Protection of national information	Data breaches can expose patron data. Data breaches can damage user trust.
	Protection of Information Assets	Protection of sensitive information Large digital collections Collection security	Weak data protection can erode trust among content submitters. Historical information about the nation needs protection.
	Information security	Importance of information security Need for security controls	Politically sensitive national information requires protection. Libraries manage vast digital collections. Digital collections must be safeguarded. Information security is essential. Security measures are necessary to prevent data loss.
Awareness and Skill Gap	Awareness gap Institutional awareness and sensitization	Knowledge gap Institutional awareness programs Non-library-specific programs	There is a lack of knowledge to protect repository data. Cybersecurity awareness campaigns are institutional.
	Lack of awareness	Low cybersecurity knowledge Low cybersecurity knowledge Limited cyber risk awareness Limited cyber threat knowledge	Cybersecurity awareness campaigns are not library-specific. There is a lack of understanding of cyber threats. There is a lack of understanding of cyber-attacks. Lack of understanding of how cyberattacks could affect the organization.
	skill gap	Data management skills Digital preservation skills Data protection skills Access control skills Data management competency Cybersecurity management skills	Lack of understanding of how cyberattacks occur. Skills in data management are needed. Skills in digital preservation are needed. Skills in data protection are needed Skills in access control are needed

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

		Technical cybersecurity skills	Data management skills are required
		Backup management skills	Managerial skills are required
		Vulnerability assessment skills	Technical skills are required
		System maintenance skills	Routine data backup skills are necessary
		Cybersecurity communication skills	Vulnerability scanning skills are necessary
		Digital content protection	Software update skills are necessary.
		Cyber threat detection skills	Communication skills are important
		Cybersecurity policy skills	Skills needed to protect online content
		Centralized cybersecurity expertise	Skills needed to recognize cyber threats
		Skills gap among librarians	Policy-making skills in cybersecurity are necessary.
		Secure storage skills	Cybersecurity skills lie mainly with systems administrators.
		Phishing detection skills	Information professionals lack cybersecurity skills.
	Knowledge gap	Regulatory knowledge	Skills in secure data storage are required.
		Incident reporting knowledge	Skills in recognizing and preventing phishing attacks.
		Security response knowledge	Knowledge of data protection regulations is needed.
		Incident response capability	Knowledge of reporting cybersecurity threats.
	Digital literacy skill	Digital literacy competence	Knowledge of responding to security breaches.
			Knowledge of responding to cyber incidents
	Low awareness	Slow awareness initiatives	Digital literacy skills are needed.
		Low cybersecurity awareness	Awareness creation on cybersecurity is slow.
			There is a lack of cybersecurity awareness
Cybersecurity Education and Capacity Building	Capacity building gap	Limited capacity building	Capacity-building opportunities are insufficient.
		Lack of training	No cybersecurity training is provided.
	Training gap	Infrequent training	Cybersecurity training is not frequent.
		One-time training	Cybersecurity training has been conducted once in the institution.
		Occasional training	Some cybersecurity training has been conducted.
	Prioritizing trainees	Selective training	Only selected staff members receive training.
	Cybersecurity education	User cybersecurity education	Librarians need skills to educate patrons on safe practices.
	Lack of training	Lack of training	
		Absence of cybersecurity curriculum	There is a lack of cybersecurity training
	Lack of cybersecurity capacity building	Limited capacity building	Cybersecurity courses are not integrated into the curriculum.
		Inadequate staff training	Capacity-building opportunities are limited.
			Staff training on cybersecurity is insufficient

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)

Institutional and Resource Barriers	Lack of resources	Insufficient funding	There is lack of funding for cybersecurity initiatives and training.
	High cost of training	High training cost	The cost of cybersecurity training is high.
	Lack of infrastructure	Lack of monitoring tools	There is lack of real-time monitoring equipment.
		Shortage of cybersecurity experts	There is lack of cybersecurity experts.
	Lack of expertise	Limited technical expertise	There is lack of cybersecurity expertise.
	Organizational priorities	Administrative priorities	University administration priorities affect cybersecurity initiatives.
		Low institutional priority	Institutional priorities limit cybersecurity initiatives.
	Lack of policy	Absence of a cybersecurity policy	There is lack of a cybersecurity policy
Indifferent Attitude of Staff toward Cybersecurity	Worker's priorities	Workload constraints	Staff struggle to balance time and workload.
	Indifferent attitude of staff	Poor cybersecurity culture	There is a mindset that cybersecurity is not our concern.
	Competing job priorities	Professional duties priorities	Cybersecurity is not within our responsibility and role

DOI: 10.1108/DLP-04-2026-0152 | License 4.0 (CC BY-NC 4.0)