PROMOTING CYBERSECURITY AWARENESS AND BEST PRACTICES IN POLYTECHNIC LIBRARIES IN DELTA AND IMO STATES.

by

Julia Chinwe Oguedoihu CLN
Ufuma Campus Library, Federal Polytechnic Oko, Anambra State, Nigeria.
chinwe.oguedoihu@fedearalpolyoko.edu.ng

and

Adaora Joy Udo-Anyanwu Ph.D, CLN
Department of Library and Information Science
Imo State University, Owerri.
dradaudo@mail.com

Abstract

This paper investigated promoting cybersecurity awareness and best practices in polytechnic libraries in Delta and Imo States. The study was guided by five research questions. The study adopted a survey research design with a population of 39 library staff, comprising 26 from the Federal Polytechnic Nekede Library, Owerri, Imo State, and 13 from the Delta State Polytechnic Library, Ogwashi-Uku, Delta State. Both professional and para-professional staff were studied using a census enumeration technique. All the 39 copies of questionnaire distributed were completed and retrieved, giving a 100% response rate. Data were collected using a rated questionnaire and analyzed using frequency counts, percentages, mean, and standard deviation. Findings revealed that library staff demonstrated a generally high level of cybersecurity awareness, particularly in password protection, safe internet practices, and identifying phishing attempts. Libraries were found to play an essential role in promoting cybersecurity awareness through workshops, user training, and digital literacy programmes. However, threats such as phishing, malware, and ransomware remain prevalent. The study further identified challenges including inadequate funding, lack of continuous training, and poor enforcement of cybersecurity policies, which limit effective awareness promotion. Strategies such as regular training, adoption of multi-factor authentication, collaboration with cybersecurity agencies, and community outreach initiatives were highlighted as necessary measures for embedding best practices. Based on these findings, the study recommends that libraries institutionalize continuous cybersecurity training for staff and users, strengthen collaborations with relevant agencies, and advocate for improved funding to enhance infrastructure and security tools. By doing so, libraries will not only safeguard their systems but also empower communities to navigate the digital environment more safely.

Keywords: Promoting, Cybersecurity, Awareness, Best Practices, Libraries.

Introduction

In today's digital era, the importance of cybersecurity cannot be overstated. As individuals, organizations, and communities increasingly depend on digital platforms for communication, learning, research, business, and social interactions, cyber threats have simultaneously become more pervasive and sophisticated. Libraries, which traditionally serve as gateways to knowledge, have not been immune to this digital transformation. The adoption of Information and Communication Technologies (ICTs) in libraries has facilitated access to electronic resources, digital repositories, and online learning platforms. However, this reliance on digital infrastructure has made both libraries and their user communities vulnerable to cyber threats such as data breaches, phishing attacks, malware infections, identity theft, and ransomware (Alotaibi, 2021). Cybersecurity awareness in libraries and communities is therefore an urgent priority. A study by Anderson and Agarwal (2020) emphasized that lack of awareness is one of the most significant contributors to the success of cyber-attacks. Many library users, including students, researchers, and community members, may unknowingly expose themselves to risks by using unsecured public Wi-Fi, mishandling passwords, or failing to recognize phishing schemes. Similarly, library staff who are not well-trained in cybersecurity best practices may inadvertently compromise systems and sensitive user data (Tella, 2022). Thus, promoting cybersecurity awareness and equipping both staff and patrons with best practices is a critical responsibility of libraries as centers of learning and community development.

Libraries play a dual role in cybersecurity awareness: as institutions safeguarding their digital systems and resources, and as educators empowering communities to navigate the digital landscape safely. As custodians of digital knowledge, libraries must implement strong data protection policies, encryption standards, and secure authentication systems. As educators, libraries are uniquely positioned to provide workshops, outreach programmes, and literacy campaigns on safe digital practices (Ifijeh & Iwu-James, 2020). These roles make libraries strategic allies in the global campaign against cybercrime. Cyber threats are not limited to large organizations; individuals and local communities are increasingly targeted. Cybercriminals exploit vulnerabilities in ordinary citizens who lack the knowledge or resources to defend themselves. Cybercrimes have had debilitating effects on individuals, governments, organizations, and universities (Adesina & Ingirige, 2019). It has cost billions of dollars' worth of damages, data loss, and website defacement. It has sent many governments, organizations, and individuals into bankruptcy and global shock (De Paoli et al., 2020). Incidents of cybercriminals have been recorded in many university libraries in Nigeria, ranging from unauthorized access to print and electronic resources in university libraries, hacking the university's library portal, computer virus, impersonation and identity theft among others. Developing countries like Nigeria are faced with challenges such as: low levels of digital literacy, limited infrastructure, and scarce cybersecurity training opportunities. Communities that rely heavily on public libraries for internet access are especially vulnerable (Okike, 2021).

Promoting cybersecurity awareness in libraries and communities is also integral to achieving the United Nations' Sustainable Development Goals (SDGs), particularly SDG 4 (quality education), SDG 9 (industry, innovation, and infrastructure), and SDG 16 (peace, justice, and strong institutions) (United Nations, 2015). By fostering cybersecurity literacy, libraries contribute to building resilient, informed, and digitally responsible societies. Moreover, cybersecurity is not just a technical issue but also a social and ethical concern. Awareness campaigns must consider cultural and contextual factors, ensuring that best practices are accessible, inclusive, and practical for diverse populations. Globally, initiatives such as Cybersecurity Awareness Month in the United States and Europe highlight the collective responsibility of individuals, organizations, and governments in combating cyber threats (Cybersecurity & Infrastructure Security Agency [CISA], 2023). Libraries and community organizations can adapt such initiatives to their local contexts, tailoring programmes to meet the needs of specific user groups—students, small business owners, researchers, or elderly citizens—who may face distinct risks online. A localized approach ensures that awareness and best practices are not abstract concepts but actionable steps for everyday digital safety (Olajide, 2022).

In academic discourse, cybersecurity is often framed in terms of technology—firewalls, intrusion detection systems, or antivirus software. While these tools are essential, human error remains the leading cause of security breaches. Richardson, Lemoine, Stephens and Waller (2020) reported that, human factor is the underlying reason why many attacks on school computers and systems are successful, thus, the need to acquire the required skills for effective and proactive cybersecurity. The awareness and behaviour of end-users be they library staff or polytechnic community members will determine the effectiveness of any cybersecurity strategy. Hence, cultivating cybersecurity awareness and best practices through libraries and community engagement is a sustainable, people-centered approach to addressing digital threats.

This study is significant in several ways. First, it contributes to the academic discussion on the intersection of cybersecurity and library science, a relatively underexplored area in research. Secondly, it highlights the role of libraries as not only repositories of knowledge but also proactive agents of digital literacy and safety. Thirdly, it provides practical strategies that libraries and communities can adopt to mitigate cyber risks. Finally, it aligns with global efforts to strengthen cybersecurity capacity across societies, particularly in regions where awareness levels remain low.

Statement of the Problem

The growing integration of digital technologies in libraries and communities has expanded access to information but has also increased vulnerability to cyber threats. Many library staff and users lack adequate cybersecurity awareness, making them susceptible to phishing attacks, data breaches, identity theft, and other cybercrimes. Although libraries are expected to safeguard digital resources and educate their communities on safe digital practices, limited training, scarce resources, and weak institutional policies often hinder these efforts. In developing countries, such as Nigeria, the situation is further compounded by low levels of digital literacy and infrastructural challenges. Without deliberate strategies to promote

cybersecurity awareness and best practices, both libraries and the communities they serve remain at risk of exploitation, thereby undermining their role as safe gateways to knowledge and community development.

Research Objectives

The general aim of this study is promoting cybersecurity awareness and best practices in polytechnic libraries and communities in Delta and Imo States. Specifically, it seeks:

1. To identify the level of cybersecurity awareness among library staff in polytechnic libraries in Delta and Imo States.
2. To identify the role of libraries in promoting cybersecurity awareness for best practices.
3. To identify the cyber threats faced by libraries in the academic community.
4. To identify the challenges libraries face in promoting cybersecurity awareness for best practices.
5. To identify strategies for the best practices of cybersecurity in the academic community.

Literature Review

Cybersecurity awareness refers to the knowledge and attitudes that individuals hold regarding the protection of information systems and data. It involves understanding potential cyber threats, recognizing vulnerabilities, and adopting safe behaviours to reduce risks (Parsons et al., 2019). In the context of libraries and communities, cybersecurity awareness is not merely about technical skills but also about cultivating responsible digital citizenship. Libraries face a range of cyber threats, including unauthorized access to library databases, malware infections through public access computers, and phishing attacks targeting both staff and patrons. Communities, particularly in developing countries, encounter similar threats due to shared ICT infrastructure, low awareness levels, and limited access to cybersecurity tools (Okike, 2021). The role of libraries in promoting digital literacy has been widely documented (Ifijeh & Yusuf, 2020), and expanding this role to include cybersecurity awareness is a logical progression. Through seminars, user training sessions, online tutorials, and public campaigns, libraries can serve as trusted platforms for cybersecurity education (Tella, 2022). Best practices in cybersecurity promotion include the implementation of strong authentication methods, regular staff training, community outreach programmes, and collaborations with government agencies or NGOs. For instance, libraries in developed countries have partnered with cybersecurity organizations to host awareness events, distribute educational materials, and provide secure internet access points (Anderson & Agarwal, 2020).

While there is a growing body of work on cybersecurity in education and business, less attention has been given to libraries and community contexts, especially in developing nations. Most studies focus on technical safeguards rather than human-centered awareness strategies. This study seeks to fill that gap by emphasizing the role of libraries in fostering cybersecurity awareness at the grassroots level. Cybersecurity awareness has emerged as a pressing global concern as libraries and communities continue to embrace digital technologies for information access, learning, and communication. Awareness in this context refers to the knowledge, attitudes, and behaviours that individuals and institutions

demonstrate in recognizing and mitigating cyber risks. In libraries, awareness is particularly critical because staff manage sensitive data, digital repositories, and networked systems accessed by a diverse user base. Panda and Kaur (2024) observed that many library professionals exhibit worrying gaps in cybersecurity awareness, with inadequate training and limited exposure to protective practices. Similarly, Aderibigbe and Owolabi (2020) found that although library and information science educators in Nigeria demonstrated relatively high awareness of cyber-ethical issues such as privacy and intellectual property, there remains a discrepancy in practical cybersecurity preparedness among practicing librarians. Globally, studies reveal that human error accounts for over 90% of breaches as validated by the report of Richardson, Lemoine, Stephens and Waller (2020) that, human factor is the underlying reason why many attacks on school computers and systems are successful, thus, the need to acquire the required skills of effective and proactive cybersecurity These findings suggest that assessing and improving the cybersecurity literacy of library staff is a crucial starting point for safeguarding both institutional and community digital resources.

The threats faced by libraries in community settings are diverse and evolving. Libraries, often seen as safe spaces, have become attractive targets for cybercriminals due to their open-access infrastructure and reliance on digital databases. Udumukwu and Nwali (2024) identified the following as types of cyber threats: malware, phishing, ransomware, denial of service attacks and insider attacks. Huang, Han, Yang and Ren (2019) found out that, computers and other online information system and infrastructures in university libraries are prone to vulnerable threats by malware agents such as viruses, trojans, adware and spyware. In academic libraries, especially in developing regions, outdated infrastructure, weak authentication systems, and inadequate staff training heighten these risks (Bellini, 2024). Threats such as phishing scams, insider misuse, and denial-of-service attacks not only compromise institutional integrity but also erode public trust in libraries as reliable centers of knowledge.

In the face of these challenges, libraries play an indispensable role in promoting cybersecurity awareness and best practices within their communities. Beyond safeguarding their own systems, libraries act as community educators and advocates of digital literacy. Ifijeh and Yusuf (2020) emphasize that libraries have historically advanced literacy, and expanding this mandate to include cybersecurity awareness is both timely and necessary. Udoh, Agbo and Osiebe (2025) advocate the use of cybersecurity management skills which are crucial in cybersecurity management, playing vital roles in ensuring effective response and mitigation of cybersecurity threats. These crucial skillsets include knowledge of network security and security technologies, including operating systems and databases; ability to know emerging threats and attack vectors, including vulnerabilities; ability to identify and respond to security incidents; ability to guide or lead cybersecurity teams and make strategic decisions; ability to plan and implement cybersecurity projects, including risk assessments and security audits. Likewise, workshops, gamified learning modules, and seminars organized by libraries have been shown to improve patrons' ability to recognize phishing attempts, protect personal data, and use public Wi-Fi securely (Uchendu et al., 2021).

Libraries, therefore, stand at the intersection of education and security, translating technical cybersecurity concepts into accessible knowledge for the general public.

Strategies for embedding cybersecurity best practices in libraries and communities must go beyond one-time interventions and embrace sustainable, context-sensitive approaches. Scholars advocate for structured, customizable training programmes that can be adapted to specific user groups and evaluated for effectiveness (Zhang & Wang, 2023). Gamification, simulation-based learning, and multimedia awareness tools have also been found to enhance user engagement and retention of cybersecurity knowledge (ACM, 2020). In addition, fostering a culture of cybersecurity within libraries requires leadership commitment, continuous professional development for staff, and the integration of security protocols into daily operations (Uchendu et al., 2021). Community-oriented strategies, such as outreach events, partnerships with NGOs and government agencies, and campaigns tailored to vulnerable groups like students and small business owners, ensure that best practices extend beyond institutional boundaries into the wider society. Ultimately, promoting best practices is not solely about deploying technical solutions but about embedding awareness, vigilance, and ethical responsibility into the community's digital culture.

The literature underscores the central role of libraries in strengthening community resilience against cyber threats. Staff awareness, institutional preparedness, and proactive outreach are interdependent elements that shape the cybersecurity landscape. While many studies highlight the threats and challenges libraries face, there remains a research gap in understanding how libraries in developing contexts, particularly in African communities, can systematically foster cybersecurity awareness and best practices. Addressing this gap is vital for ensuring that libraries continue to serve as secure, trusted, and transformative spaces in the digital era.

Omoike and Alabi (2023) investigated awareness and perception of cybersecurity among librarians in federal universities in South West, Nigeria. The study revealed that the level of awareness of cybersecurity among librarians in Federal Universities in South-West, Nigeria is moderate. The findings also revealed that to a high extent are librarians in federal universities in SouthWest, Nigeria are aware of the potential cyber threats and attacks to library resources. The study showed that librarians perceived that deliberate attack to destroy sensitive data in the library database is unjust, the use of the computer in committing crimes is unjust and that having an unauthorized access to data and other computerized systems (hacking) is considered unjust. The study revealed that hardware skill, software skill, operating system skills and programming language skills were the main librarians' information technology skills to secure library resources. The study further showed that librarians make use of technical security measures in the libraries through access control and password security, through video surveillance (CCTV system) and through installation of updated software; and the use of non-technical security measures in libraries are through burglary protection and fire extinguishers and architectural considerations. The study also showed that crashing of a computer due to virus, malware, hackers etc., lack of fund and lack of trained information technology (IT) manpower were the main challenges encountered in securing information resources against cyber-attacks by librarians. There is

no significant relationship between awareness and perception of cybersecurity among librarians in Federal Universities in South-West Nigeria.

Obim and Akpokurerie (2023) examined the Cybersecurity awareness among Librarians for effective storage of information in university libraries in Southeastern Nigeria. The findings revealed that, the major cybersecurity threats in university libraries were hacking, impersonation, interception of electronic message, unauthorized access to information resources, computer virus among others. The cybersecurity competency among librarians for effective information storage is low, which is due to inadequate training of librarians on cybersecurity measures, substandard technological infrastructures, lack of cybersecurity policy framework in university libraries among others.

Udoh, Agbo and Osiebe (2025) examined cybersecurity management skills as determinant of effective digital library services provision in public university libraries in some states in Southern Nigeria. The study revealed that librarians' level of awareness of cybersecurity management issues was relatively high on basic issues such as managing cybersecurity budgets and projects, etc., and low on issues of technical nature such as designing and developing cybersecurity architecture for digital library systems, etc. It indicated that the cybersecurity management skills required by librarians for effective digital library services provision are categorized into technical skills (such as knowledge in identifying and mitigating an attempt to hack library server to secure digital library services, ability to install and update computer virus for digital library services provision, etc.); managerial skills (like the ability to lead highly motivated teams in dealing with cybersecurity threats for digital library services provision; knowledge in effective collaboration with various departments and stakeholders in cybersecurity situation for digital library services, etc.); and soft skills (such as ability to make proactive decisions about cybersecurity issues, learn new skills about cybersecurity, and think critically in evaluating cybersecurity information for digital library services, among others). It identified rapid pace of technological evolution, general low level of librarians' skills in digital technologies, lack of cybersecurity courses in LIS curriculum, lack of tailor-made training programmes for librarians on cybersecurity issues, etc., as the major factors militating against the acquisition of cybersecurity management skills by librarians for effective digital library services provision.

Methodology

This study adopted a survey research design. The population comprised 39 library staff, made up of 26 from the Federal Polytechnic Nekede Library, Owerri, Imo State, and 13 from the Delta State Polytechnic Library, Ogwashi-Uku, Delta State. Both professional and para-professional staff formed the study population. A total of 39 copies of questionnaire were distributed, and all were successfully retrieved, representing a 100% response rate. The study employed total enumeration, thereby covering the entire population of library staff in the two institutions. Data were collected using a structured questionnaire designed on a 4-point Likert scale of Strongly Agree (4), Agree (3), Disagree (2), and Strongly Disagree (1). The collected data were analyzed using frequency counts, percentages, mean, and standard

deviation. The interpretation of mean scores was guided by the following decision rule: 3.25 – 4.00 = Very High, 2.50 – 3.24 = High, 1.75 – 2.49 = Low, and 1.00 – 1.74 = Very Low.

Presentation of Result

Table 1: The Level of Cybersecurity Awareness among Library Staff in the Polytechnic Libraries

S/N	Item Statements	SA f(%)	A f(%)	D f(%)	SD f(%)	Mean	SD	Rem
1	I am aware of phishing attacks targeting libraries	15 (38.5%)	12 (30.8%)	8 (20.5%)	4 (10.2%)	2.98	0.92	High
2	I understand the importance of using strong passwords	20 (51.3%)	10 (25.6%)	6 (15.4%)	3 (7.7%)	3.18	0.92	High
3	I regularly update my library system credentials	8 (20.5%)	12 (30.8%)	14 (35.9%)	5 (12.8%)	2.49	0.98	Low
4	I can identify malware or suspicious attachments in emails	6 (15.4%)	10 (25.6%)	15 (38.5%)	8 (20.5%)	2.21	0.96	Low
5	I follow protocols for securing library data	18 (46.2%)	10 (25.6%)	8 (20.5%)	3 (7.7%)	3.15	0.94	High
6	I understand the importance of encryption for sensitive data	5 (12.8%)	8 (20.5%)	16 (41.0%)	10 (25.7%)	1.97	0.93	Low
7	I have attended cybersecurity awareness training in the past year	3 (7.7%)	7 (17.9%)	15 (38.5%)	14 (35.9%)	1.79	0.88	Low
	Grand mean					2.54	0.93	High

The results show variation in cybersecurity awareness among library staff. The level of awareness of on phishing attacks (2.98), understanding the importance of strong passwords (3.18) and securing library data (3.15) are high; their level of awareness of library system credentials (2.49), identifying malware or suspicious attachments in emails (2.21), encryption for sensitive data (1.97) and attendance to cybersecurity awareness training in the past year (1.79) is low. This indicates gaps in practical preparedness, highlighting the need for targeted awareness and hands-on training. Generally, there is a high level of awareness as can be seen in the grand mean.

Table 2: The Role of Libraries in Promoting Cybersecurity Awareness in the Polytechnic for Best Practices

S/N	Item Statements	SA f(%)	A f(%)	D f(%)	SD f(%)	Mean	SD	Rem
1	Libraries organize workshops on safe internet use	12 (30.8%)	10 (25.6%)	9 (23.1%)	8 (20.5%)	2.59	1.01	High
2	Libraries provide online resources on cyber security	10 (25.6%)	12 (30.8%)	10 (25.6%)	7 (17.9%)	2.59	0.95	High
3	Libraries train community members to recognize phishing attempts	6 (15.4%)	11 (28.2%)	14 (35.9%)	8 (20.5%)	2.21	0.93	Low
4	Libraries create awareness campaigns through social media	5 (12.8%)	9 (23.1%)	15 (38.5%)	10 (25.6%)	1.97	0.92	Low
5	Libraries collaborate with schools and organizations	7 (17.9%)	12 (30.8%)	13 (33.3%)	7 (18.0%)	2.31	0.89	Low

6	Libraries provide guidance on password management to users	14 (35.9%)	9 (23.1%)	10 (25.6%)	6 (15.4%)	2.69	0.95	High
7	Libraries actively promote ethical digital practices	15 (38.5%)	10 (25.6%)	9 (23.1%)	5 (12.8%)	2.82	0.92	High

The analysis indicates that libraries play some active roles in promoting cybersecurity. Ranking highest promotion of ethical digital practice (2.83), followed by provision of guidance on password management to users (2.69), organizing workshops on safe internet use (2.59), and provision of online resources on cyber security (2.59). However, training community members to recognize phishing attempts (2.21), creating awareness campaigns through social media (1.97) and collaborating with schools and organizations (2.31)

Table 3: The Cyber Threats Faced by the Polytechnic Libraries

S/N	Item Statements	SA f(%)	A f(%)	D f(%)	SD f(%)	Mean	SD	Rem
1	Libraries face phishing attacks targeting users	14 (35.9%)	11 (28.2%)	9 (23.1%)	5 (12.8%)	2.77	0.97	High
2	Libraries experience malware infections on public access computers	10 (25.6%)	12 (30.8%)	10 (25.6%)	7 (17.9%)	2.59	0.95	High
3	Libraries are vulnerable to ransomware attacks	6 (15.4%)	11 (28.2%)	14 (35.9%)	8 (20.5%)	2.21	0.93	Low
4	Users unintentionally expose library systems to threats	8 (20.5%)	12 (30.8%)	13 (33.3%)	6 (15.4%)	2.36	0.88	Low

5	Insider threats from staff pose cybersecurity risks	5 (12.8%)	10 (25.6%)	15 (38.5%)	9 (23.1%)	1.92	0.91	Low
6	Libraries face denial-of-service attempts	4 (10.2%)	9 (23.1%)	16 (41.0%)	10 (25.7%)	1.79	0.87	Low
7	Weak authentication systems increase vulnerability	7 (17.9%)	10 (25.6%)	13 (33.3%)	9 (23.1%)	2.08	0.88	Low

The analysis show that Phishing and malware are the most recognized threats as can be shown by their mean scores of 2.77 and 2.59 respectively which are above the criterion mean of 2.50. Ransomware (2.21), users unintentionally expose library systems to threats (2.36), insider threats (1.92), denial-of-service attempts (1.79) and weak authentication (2.08) are lowly acknowledged as threats. This indicates that staff may underestimate serious or technical threats, which could compromise library systems.

Table 4: The Challenges Libraries face in Promoting Cybersecurity Awareness for Best Practices.

S/N	Item Statements	SA f(%)	A f(%)	D f(%)	SD f(%)	Mean	SD	Rem
1	Lack of funding for cybersecurity programmes	12 (30.8%)	10 (25.6%)	10 (25.6%)	7 (17.9%)	2.54	0.98	High
2	Inadequate training for library staff	9 (23.1%)	11 (28.2%)	12 (30.8%)	7 (17.9%)	2.36	0.95	Low
3	Low digital literacy of staff	15 (38.5%)	10 (25.6%)	9 (23.1%)	5 (12.8%)	2.82	0.94	High
4	Limited access to modern cybersecurity tools	7 (17.9%)	12 (30.8%)	13 (33.3%)	7 (18.0%)	2.23	0.91	Low

5	Resistance to adopting security policies	6 (15.4%)	9 (23.1%)	15 (38.5%)	9 (23.1%)	1.90	0.88	Low
6	Lack of collaboration with external agencies	5 (12.8%)	11 (28.2%)	14 (35.9%)	9 (23.1%)	1.92	0.89	Low
7	Time constraints for community outreach programs	8 (20.5%)	10 (25.6%)	14 (35.9%)	7 (17.9%)	2.15	0.87	Low

The table above shows that the top challenges that libraries face in promoting cybersecurity awareness are lack of funding for cybersecurity programmes (2.54) and low digital literacy of staff (2.82), while inadequate training for library staff (2.36), limited access to modern cybersecurity tools (2.23), resistance to adopting security policies (1.90), lack of collaboration with external agencies (1.92) and time constraints for community outreach programs (2.15) are low showing that they are not seen as challenges that libraries face in promoting cybersecurity awareness.

Table 5: Strategies for the Best Practices of Cybersecurity in the Library

S/N	**Item Statements**	**SA f(%)**	**A f(%)**	**D f(%)**	**SD f(%)**	**Mean**	**SD**	**Rem**
1	Conduct regular cybersecurity workshops for staff.	16 (41.0%)	10 (25.6%)	8 (20.5%)	5 (12.8%)	2.87	0.99	High
2	Provide online tutorials and guides on cybersecurity	10 (25.6%)	12 (30.8%)	11 (28.2%)	6 (15.4%)	2.49	0.95	Low
3	Collaborate with cybersecurity organizations	8 (20.5%)	11 (28.2%)	13 (33.3%)	7 (17.9%)	2.21	0.91	Low
4	Implement multi-factor authentication for library systems	6 (15.4%)	10 (25.6%)	15 (38.5%)	8 (20.5%)	1.97	0.89	Low

5	Regularly update library systems and software	14 (35.9 %)	11 (28.2 %)	8 (20.5 %)	6 (15.4 %)	2.69	0.92	High
6	Encourage library staff to adopt safe digital practices	17 (43.6 %)	10 (25.6 %)	7 (17.9 %)	5 (12.8 %)	2.92	0.91	High
7	Monitor and review cybersecurity policies periodically	7 (17.9 %)	12 (30.8 %)	13 (33.3 %)	7 (18.0 %)	2.21	0.90	Low

The analysis in the Table 5 above show that the strategies rated high for the best practices of cybersecurity in the library include: conducting regular cybersecurity workshops for staff (2.87)., regular update of library systems and software (2.69) and encouraging library staff to adopt safe digital practices (2.93). Provision of online tutorials and guides on cybersecurity (2.49), collaboration with organizations (2.21), implementation of multi-factor authentication for library systems (1.97) and monitoring and reviewing cybersecurity policies periodically (2.21) were rated low.

Discussion of Findings

The analysis revealed varied levels of cybersecurity awareness among library staff, with some staff demonstrating high awareness regarding phishing attacks and strong passwords, while other aspects, such as encryption and attendance of cybersecurity training, were rated low. This aligns with the findings of Udoh, Agbo and Osiebe (2025) that librarians' level of awareness of cybersecurity management issues was relatively high on basic issues such as managing cybersecurity budgets and projects, etc., and low on issues of technical nature such as designing and developing cybersecurity architecture for digital library systems, etc. Similarly, Aderibigbe and Owolabi (2020) emphasized that while Nigerian library educators show awareness of cyber-ethical issues, there is a discrepancy between theoretical knowledge and hands-on application. The finding also supports that of Anderson and Agarwal (2020) who emphasized that lack of awareness is one of the most significant contributors to the success of cyber-attacks. Many library users, including students, researchers, and community members, may unknowingly expose themselves to risks by using unsecured public Wi-Fi, mishandling passwords, or failing to recognize phishing schemes. This finding does not corroborate with that of Omoike and Alabi (2023) that there is no significant relationship between awareness and perception of cybersecurity among librarians in Federal Universities in South-West Nigeria.

The findings indicated that libraries actively conduct workshops and promote ethical practices, but social media campaigns, school collaborations, and broader community

outreach were rated low. This is in agreement with Okike (2021), who observed that while libraries have the potential to educate communities, their outreach often remains limited in developing countries due to infrastructural and resource constraints. Ifijeh and Iwu-James (2020) also emphasized that libraries are uniquely positioned to act as educators and digital literacy hubs, but systematic and consistent programming is essential for maximum impact. Uchendu et al. (2021) also emphasized that workshops, gamified learning modules, and seminars organized by libraries have been shown to improve patrons' ability to recognize phishing attempts, protect personal data, and use public Wi-Fi securely.

The study found that phishing and malware attacks were the most recognized threats, while ransomware, insider threats, weak authentication, and denial-of-service attempts were rated low. The finding differs from that of Obim and Akpokurerie (2023) that the major cybersecurity threats in university libraries were hacking, impersonation, interception of electronic message, unauthorized access to information resources, computer virus among others. Okiki (2021) identified that libraries face a range of cyber threats, including unauthorized access to library databases, malware infections through public access computers, and phishing attacks targeting both staff and patrons. These threats not only compromise systems but also erode public trust in libraries as secure knowledge centers. Udumukwu and Nwali (2024) also identified the following as types of cyber threats: malware, phishing, ransomware, denial of service attacks and insider attacks.

Challenges identified include: lack of funding, low digital literacy among community members, limited staff training, and poor collaboration with external agencies. Funding and low literacy were rated High, while other factors were Low. These findings are consistent with Zhang and Wang. (2023), who noted that resource constraints and lack of technical capacity are major barriers to effective cybersecurity programmes in educational and community settings. Similarly, Uchendu et al. (2021) highlighted that staff knowledge gaps, infrastructural limitations, and low community engagement hinder sustainable cybersecurity awareness initiatives. Omoike and Alabi (2023) also identified lack of fund and lack of trained information technology (IT) manpower as the main challenges encountered in securing information resources against cyber attacks by librarians.

The analysis showed that practical strategies such as workshops, updating systems, and encouraging safe digital practices were rated high, while technical strategies like multi-factor authentication and organizational collaboration were Low. Zhang and Wang. (2023) advocated that strategies for embedding cybersecurity best practices in libraries and communities must go beyond one-time interventions and embrace sustainable, context-sensitive approaches. Scholars advocate for structured, customizable training programmes that can be adapted to specific user groups and evaluated for effectiveness. Uchendu et al. (2021) opined that fostering a culture of cybersecurity within libraries requires leadership commitment, continuous professional development for staff, and the integration of security protocols into daily operations. The study indicates that while libraries prioritize practical interventions, the adoption of technical measures remains limited.

Conclusion

The findings of this study underscore the relevant roles that libraries play in promoting cybersecurity awareness and best practices within their communities. Libraries are not only custodians of digital knowledge but also crucial agents in educating users on safe and responsible digital behaviour. The study revealed that while some library staff possess a high level of awareness of basic cybersecurity concepts, but the problem lies in practical knowledge, training, and preparedness for emerging cyber threats. This aligns with global observations that human error and inadequate training continue to be leading contributors to cybersecurity breaches.

Libraries, therefore, must balance technicalities with people-centered approaches, ensuring that awareness translates into actionable behaviors among staff and the polytechnic community users. This requires the efforts of all the stakeholders through staff capacity-building, community engagement, infrastructure development, and policy implementation. Ultimately, strengthening cybersecurity awareness through libraries contributes not only to the protection of information systems but also to the creation of resilient, informed, and digitally responsible communities, supporting broader national and global development goal.

Recommendations

Based on the findings, it was recommended that:

1. Libraries should implement structured, periodic cybersecurity training programmes for library staff, focusing on malware detection, encryption, phishing simulations, and practical system security. This will improve low-awareness areas and strengthen institutional cybersecurity practices.
2. Libraries should strengthen partnerships with schools, NGOs, and local authorities and expand their outreach through social media campaigns, ensuring structured and continuous community engagement for cybersecurity awareness consistently.
3. Libraries should implement a comprehensive cybersecurity risk management plan, including system updates, malware protection, multi-factor authentication, and insider threat monitoring, to mitigate potential vulnerabilities effectively.
4. Libraries should seek funding support, from strategic partnerships, and implement staff capacity-building programs to overcome resource and knowledge barriers and facilitate effective community cybersecurity awareness initiatives.
5. Libraries should prioritize practical, community-oriented strategies such as workshops, training, and safe digital practices while gradually integrating technical measures and organizational collaborations to ensure comprehensive cybersecurity best practices.

References

Aderibigbe, O., & Owolabi, J. (2020). Cybersecurity preparedness among Nigerian library staff. *Library Philosophy and Practice.* https://digitalcommons.unl.edu/libphilprac/.

Adesina, R., & Ingirige, B. (2019). Dismantling barriers to effective disaster management in Nigeria. 14th International Postgraduate research conference 2019: Contemporary and Future Directions in the Built Environment,

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M., & Martin,R. (2020). A Qualitative Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists. *Policing: A Journal of Policy and Practice.*

ACM. (2020). *Enhancing cybersecurity awareness through educational tools. Association for Computing Machinery. https://www.acm.org/.*

Alotaibi, F. (2021). Cybersecurity awareness in academic libraries. *Journal of Information Security,* 12(3), 45–60. https://doi.org/10.1007/s10207-021-00512-3

Anderson, C., & Agarwal, R. (2020). The role of awareness in cybersecurity defense. *Computers & Security,* 92, 101751. *https://doi.org/10.1016/j.cose.2020.101751.*

Bellini, P. (2024). Cybersecurity threats in community libraries. *International Journal of Library and Information Science,* 16(2), 67–79. *https://doi.org/10.5897/IJLIS2024.016.*

Cybersecurity and Infrastructure Security Agency CISA (2024). Cybersecurity Awareness Month toolkit/resources. *Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/cybersecurity-awareness-month.*

Huang, S., Han, Z., Yang, Bo, & Ren, Ni (2019b). Factor identification and computation in the assessment of information security risks for digital libraries. *Journal of Librarianship & Information Science, 51* (1), 78–94.

Ifijeh, G., & Iwu-James, A. (2020). Libraries as community digital literacy hubs. *African Journal of Library, Archives, and Information Science*, 30(1), 55–68. *https://ajlais.org/.*

Ifijeh, G., & Yusuf, F. (2020). COVID–19 pandemic and the future of Nigeria's university system: The quest for libraries' relevance. *Journal of Academic Librarianship*, 46(6), 102226. *https://doi.org/10.1016/j.acalib.2020.102226.*

Obim, I. E. & Akpokurerie, A. O. (2023) examined the Cybersecurity awareness among Librarians for effective storage of information in university libraries in Southeastern Nigeria. *Information Technology and Librarianship: Journal of NLA IT Section*, 3 (2), 126-140.

Olajide, T. (2022). Cybersecurity awareness and sustainable development in Africa. *Journal of African Digital Studies, 4*(2), 88–102.

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

Okike, E. (2021). Promoting cybersecurity awareness in developing countries. Information Development, 37(4), 625–634. *https://doi.org/10.1177/02666669211012456.*

Panda, S., & Kaur, R. (2024). Cybersecurity literacy among library professionals: A global review. *Journal of Academic Librarianship,* 50(1), 101–112. *https://doi.org/10.1016/j.acalib.2024.101112.*

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2019). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. *https://doi.org/10.1016/j.cose.2013.12.003.*

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cybersecurity in schools: the human factor. *Educational Planning*, 27(2), 23-39.

Tella, A. (2022). The role of Nigerian libraries in promoting cybersecurity awareness. *Library Philosophy and Practice.* . https://digitalcommons.unl.edu/libphilprac/.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). *Developing a cyber security culture: Current practices and future needs. arXiv. https://arxiv.org/abs/2106.14701*.

Udoh, I. U., Agbo, A. D. & Osiebe, P. O. (2025). Cybersecurity management skills as determinant of effective digital library services provision in public university libraries in some states in Southern Nigeria. *Library and Information Perspectives and Research*, 7(3), 98 – 120.

Udumukwu and Nwali (2024). Cybersecurity and privacy in federal university libraries in Nigeria. *Journal of Applied Information Science and Technology*, 17 (2), 107-120.

United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development. United Nations. https://sdgs.un.org/2030agenda*.

Zhang, Y., Li, X., & Wang, H. (2023). Sustainable cybersecurity education strategies for communities. *Computers & Education*, 192, 104686. *https://doi.org/10.1016/j.compedu.2022.104686.*