FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 12, December, 2025, pp 9 – 19
DOI: https://doi.org/10.33003/fjs-2025-0912-3990

PERSPECTIVES OF LIBRARIANS ON THE IMPACT OF CYBER THREATS IN THE MANAGEMENT OF DIGITAL LIBRARIES IN KWARA STATE, NIGERIA

***[1]Idris, Olanrewaju Ibraheem, [1]Yusuf, Abdullahi Adebola, [1]Bolakale, Lawal Aremu and [2]Muhammad Tijjani Jidda**

[1]Al-Hikmah University Ilorin, Nigeria.
[2]Ahmadu Bello University Zaria, Nigeria.

*Corresponding authors' email: ioibraheem@alhikmah.edu.ng

ABSTRACT

This study examines the perspectives of librarians on the impact of cyber threats in managing digital libraries in Nigeria within the context of the Fifth Industrial Revolution. As digital libraries expand, they face growing risks such as data breaches, ransomware, and phishing, which threaten their integrity and accessibility. Data was collected through surveys administered to digital library professionals and analyzed using Python-based tools, including descriptive statistics, comparative tests, and a Random Forest model. The analysis revealed that cyber threats are perceived as more disruptive in public libraries than in academic ones. Public libraries prioritize data encryption, while academic libraries emphasize access control and regular software updates. Confidence in managing cyber threats varies with experience, as less experienced staff report high confidence but moderate familiarity. The Random Forest model achieved 95% accuracy, confirming that experience, library type, and security measures predict threat exposure. The findings emphasize the need for continuous cybersecurity training and tailored defense strategies to enhance digital library resilience in Nigeria.

Keywords: Cyberthreats, Digital libraries, librarians' perspectives, Cybersecurity Management, Data Protection

INTRODUCTION

In the rapidly evolving landscape of the Fifth Industrial Revolution, digital libraries stand as pivotal repositories of knowledge, facilitating the seamless exchange of information across borders and disciplines. As these digital repositories become increasingly indispensable in the dissemination and preservation of scholarly works, educational resources, and cultural artifacts, they also become prime targets for malicious cyber activities. The convergence of the digital era with the proliferation of cyber threats presents a pressing challenge for the effective management of digital libraries. However, digital libraries, characterized by their vast collections of digital assets, offer unparalleled accessibility and scalability, transcending geographical and temporal boundaries. They serve diverse user populations ranging from researchers and students to professionals and the public, catering to a spectrum of informational needs (Mani, 2023). Alongside their transformative potential, digital libraries are confronted with an array of cyber threats that jeopardize the integrity, confidentiality, and availability of their resources.

In contemporary digital library environments, cybersecurity has become a central component of information management. The integration of new technologies such as artificial intelligence and cloud computing has reshaped how data is handled but at the same time expanded the attack surface for cybercriminals. Hence, understanding the impact of cyber threats within digital library management requires an appreciation of both technological and managerial frameworks that govern secure information dissemination (Oladokun et al, 2022). Cyber threats manifest in various forms, including but not limited to data breaches, ransomware attacks, phishing scams, and distributed denial-of-service (DDoS) assaults. These threats exploit vulnerabilities within digital systems and networks, posing significant risks to the reliability and security of digital library platforms (Jony & Hamim, 2023). Moreover, the constantly evolving nature of cyber threats complicates the task of digital library managers, necessitating proactive measures to mitigate potential damage. By exploring the nuanced interplay between cyber threats and digital library management, this study seeks to explore the perspectives of librarians on the multifaceted impact of cyber threats on digital library management.

The study aims to explore the perspectives of librarians on the impact of cyber threats on the management of digital libraries within the context of the Fifth Industrial Revolution by exploring the perspective of librarian on how cyber threats affect the management of digital libraries, explore how librarians view the effects of cyber threats on the management of digital libraries, explore the cyber threats inherent in digital library systems and networks, and explore effective methods to reduce cyber threats in the management of digital libraries.

Literature Review

Libraries serve as crucial societal institutions, providing a multitude of services and resources essential for research, education, and community engagement. With over 171 million registered public library users in the U.S. in 2016, libraries play a significant role in fostering open inquiry and preserving user privacy (Rosa & Storey, 2016). The ALA emphasizes the ethical imperative of unrestricted access to information while safeguarding against impediments to open inquiry. Fundamental to this ethos is the protection of patron privacy, as outlined in ALA's policy on the confidentiality of personally identifiable information (PII) about library users (McMenemy, 2023). This confidentiality extends to various aspects of patron interactions with library resources and services, underscoring the importance of maintaining patron privacy to uphold the freedom of inquiry within libraries (Parme, 2023).

Despite the recognized importance of data protection, librarians often lack resources and expertise to assess information security risks and implement mitigation strategies effectively. With libraries increasingly accessing databases containing proprietary and personal information, the need for robust information security practices becomes imperative (Jaeger & Taylor, 2020). However, there is a notable gap in research concerning information security practices within libraries, despite the critical role of patron

privacy in librarianship and the evolving technological landscape (Farid et al, 2023). One approach to addressing this gap is through cybersecurity education, which equips library staff with the knowledge and skills necessary to identify risks and implement effective security measures. Such education can empower librarians to protect the information and resources entrusted to them while fostering a culture of security awareness within library environments (Diseiye, 2023).

In a study conducted by Ghimire (2023) on Cyber-Attack Issues: Laws & Policies and the Role of Librarians. The study explores the multifaceted landscape of cybersecurity, focusing on the deployment of people, policies, processes, and technologies to safeguard organizations, critical systems, and sensitive information from digital attacks. The study underscores the increasing vulnerability of organizations to cyber threats due to the pervasive integration of digital information and technology into daily operations. Moreover, it highlights the escalating sophistication of cyber-attacks targeting both information assets and critical infrastructure. Particularly the study aimed to delineate the major attributes of cyber-attacks, identify common cyber threats prevalent in Nepal and its surrounding regions, examine laws and policies related to cybersecurity in Nepal, and propose strategies for fostering a cyber-safe academic environment. According to Saidu et al (2021) Nigeria has moved from being the fifth most attacked country in terms of mobile malware attacks in 2017 to being the third most hit in 2018

Librarians play a pivotal role in understanding and addressing the effects of cyber threats on the management of digital libraries. Accessibility, ease of use, and perceived utility are fundamental factors influencing the utilization of information sources, including digital libraries (Kibithe & Naibei, 2023). Digital technology has revolutionized these factors, breaking down traditional barriers to access imposed by physical libraries. However, the increased accessibility facilitated by digital technology has also made digital libraries vulnerable to cyber threats, raising concerns among librarians about the security and reliability of digital resources (Akor et al, 2024). Librarians recognize the importance of distinguishing between access and actual usage in assessing the effectiveness of digital library services. While extensive visit statistics may indicate high levels of engagement, the utility and usefulness of digital resources must be carefully evaluated to ensure meaningful outcomes for users. Moreover, the prevalence of abusive practices such as click fraud in online platforms highlights the need for vigilant monitoring and authentication mechanisms to combat fraudulent activities in the use of digital library with many users with individual motives (Leguina et al, 2023).

The ease of use of digital library resources varies depending on users' information consumption skills and levels of information literacy (Oseghale, 2023). Librarians play a crucial role in promoting information literacy and providing guidance to users in navigating complex digital environments. Effective utilization of digital library resources requires not only technical proficiency but also critical thinking skills to evaluate the credibility and relevance of information (Oseghale, 2023). Perceived utility, influenced by users' trust in digital services of the library, may not always align with the actual quality and reliability of information sources. While digital environments are often perceived as trustworthy, librarians must be vigilant in ensuring the accuracy and integrity of digital resources to maintain users' confidence (Gupta et al, 2018).

The proliferation of digital content, including gray literature, presents both opportunities and challenges for digital libraries. While digital technologies have facilitated access to a vast array of information resources, librarians face challenges in managing and preserving these resources effectively. The emergence of content boom in digital form underscores the need for librarians to adopt proactive strategies for curating and disseminating digital content while addressing issues related to quality control and preservation (Pasqui, 2024).

Digital libraries play a crucial role in providing access to vast collections of information resources. However, with the proliferation of digital content, cyber threats pose significant challenges to the security and integrity of these systems. Hacking represents a prevalent cyber threat to digital library systems. Hackers exploit vulnerabilities in software or network infrastructure to gain unauthorized access to sensitive information stored in digital libraries (Parn & Edwards, 2019). This unauthorized access can lead to data breaches, manipulation of records, and disruption of library services, undermining the trust and reliability of digital collections. Unauthorized access to the illegitimate entry into digital library systems or resources without proper authorization. It encompasses various activities, including unauthorized viewing, modification, or extraction of digital content (Omotunde & Ahmed, 2023). Unauthorized access can occur through exploitation of system vulnerabilities, weak authentication mechanisms, or insider threats, undermining the security posture of digital libraries. Several factors contribute to the occurrence of unauthorized access in digital library systems. Weak access controls, inadequate encryption, and insufficient monitoring mechanisms create opportunities for malicious actors to exploit vulnerabilities (Aslan et al., 2023).

Insider Attacks Insider attacks pose a unique challenge to the security of digital libraries. Employees with privileged access to library systems may abuse their authority to compromise data integrity or steal valuable information. These insider threats can be difficult to detect and mitigate, emphasizing the importance of robust access controls and monitoring mechanisms within digital library environments (Nafea and Almaiah, 2021).

Malware and viruses present persistent threats to the integrity and availability of digital library resources. Cybercriminals deploy malicious software to infect digital systems, leading to data corruption, unauthorized access, and system downtime (Nnenda & Aforomo, 2023). The spread of malware within digital library networks can result in widespread damage and compromise the confidentiality of sensitive materials.

Data Loss Cyber threats can contribute to data loss in digital library systems, jeopardizing the preservation and accessibility of valuable collections. Inadequate backup procedures, coupled with vulnerabilities in storage infrastructure, increase the risk of data loss due to cyber incidents. The loss of digital assets not only undermines the credibility of digital libraries but also hampers scholarly research and knowledge dissemination efforts (Chickombe & Maina 2021).

In the Study (Ajie, 2019) on A Review of Trends and Issues of Cybersecurity in Academic Libraries provides a comprehensive analysis of the challenges and trends related to cybersecurity in academic libraries. The study emphasizes the importance of cyber security in protecting the valuable information resources of academic institutions. The study delves into the evolving nature of cyber threats, the impact of cybercrime on academic libraries, and the need for a holistic approach to combat these challenges. The study highlights the increasing interconnectedness of the world and the critical role that networks play in facilitating transactions within

academic libraries. The study underscores the continuous evolution of cyber threats and the emergence of disruptive technologies that pose new challenges to securing information resources. The study emphasizes the need for academic libraries to adapt to these changing landscapes by implementing new platforms and intelligence to enhance cybersecurity measures.

Furthermore, the study acknowledges that while there may not be a perfect solution to cybercrimes, efforts should be made to minimize these threats to ensure a safe and secure cyber space for academic institutions. The study recommends a holistic approach to combat cybercrime, including the establishment of institutional frameworks for monitoring information security, improving awareness and competence in cybersecurity, safeguarding privacy rights, and formalizing cyber security evaluation programs (Ajie, 2019)

Exploring effective methods to reduce cyber threats in the management of digital libraries, it is essential to consider the vulnerabilities and challenges associated with scholarly digital libraries.

Exploitation of Scholarly Digital Libraries: Attackers leverage the trust and perceived safety of scholarly digital libraries to distribute malicious PDF documents. These libraries, considered secure and harmless traditionally, can be maliciously used as platforms for malware distribution and targeted cyber security attacks. This exploitation poses a significant cyber threat to users accessing articles in these libraries (Nissim et al, 2016). Collaborative Research and Industry Partnerships: (Nissim et al, 2017), with expertise in information systems security and machine learning, lead collaborative projects between academia and industry to address cyber security challenges. Collaborations between academic institutions, industry partners, and cyber security experts can facilitate the development of innovative solutions to reduce cyber threats in digital libraries.

One key method to mitigate cyber threats is the development of a comprehensive cybersecurity policy that outlines guidelines, procedures, and responsibilities related to cybersecurity. This policy should cover areas such as data protection, access controls, network security, and incident response. By establishing clear guidelines and responsibilities, academic libraries can create a structured approach to cybersecurity management. Encryption and the use of secure protocols are essential methods to protect sensitive data and communications from unauthorized access. Implementing robust encryption algorithms and secure protocols like HTTPS can safeguard data during transmission, reducing the risk of interception by malicious actors. By encrypting data and communications, academic libraries can enhance the confidentiality and integrity of their digital collections (Aregbesola & Nwaolise 2023). Regularly updating and patching software applications, operating systems, and security solutions is another effective method to reduce cyber threats in digital libraries (Aregbesola & Nwaolise 2023). Outdated software can be vulnerable to cyberattacks, making it essential for libraries to stay current with software updates to address known vulnerabilities. By maintaining up-to-date software, libraries can strengthen their defenses against potential cyber threats.

Implementing strong user access controls, such as role-based access control (RBAC), is crucial for limiting user privileges and preventing unauthorized access to digital collections (Aregbesola & Nwaolise 2023). By assigning access rights based on job responsibilities and regularly reviewing user accounts, academic libraries can reduce the risk of unauthorized access and data breaches. User access controls play a vital role in maintaining the security and confidentiality of digital assets within libraries. Conducting regular security assessments and audits is a proactive method to identify vulnerabilities and weaknesses in the library's systems and infrastructure (Aregbesola & Nwaolise 2023). Vulnerability scanning, penetration testing, and security risk assessments can help libraries identify potential security gaps and address them promptly. By conducting periodic security assessments, academic libraries can proactively identify and mitigate cyber threats before they escalate.

Developing an incident response plan is essential for academic libraries to effectively respond to cybersecurity incidents. This plan should outline the steps to be taken in case of a security breach, including procedures for reporting incidents, containing damage, and recovering normal operations. Regularly testing and updating the incident response plan ensures that libraries are prepared to handle cyber threats effectively (Falowo et al, 2023). Collaborating with other institutions, cybersecurity experts, and relevant stakeholders is a valuable method for academic libraries to enhance their cybersecurity posture. By sharing information, best practices, and lessons learned, libraries can benefit from collective knowledge and expertise in cybersecurity. Establishing partnerships and collaborations with external entities can provide libraries with additional resources and support to strengthen their cybersecurity measures (Oladokum et al, 2023).

MATERIALS AND METHODS

The study adopted a descriptive survey design aimed at exploring the perspectives of librarians on the impact of cyber threats on digital library management in Kwara State, Nigeria. A structured questionnaire was created using Google Forms and distributed electronically through WhatsApp groups and email lists of librarians and digital librarians. A total of 105 valid responses were received and used for the analysis.

Data Collection

The questionnaire comprised sections on demographic information, awareness of cyber threats, perceived impacts, and mitigation practices. Respondents included librarians from both academic and public libraries across Kwara State. The responses were automatically captured in a spreadsheet format and subsequently exported into Python for data preprocessing and analysis.

Data Analysis Tools

Data analysis was conducted using the Python programming environment on Google Colab. The following libraries were employed for the study. Pandas and NumPy libraries were used for data cleaning and manipulation, Matplotlib was used for data visualization, SciPy for statistical and comparative analyses, and Scikit-learn for predictive modeling.

Analytical Procedures

Three major analyses were conducted

Descriptive Analysis

Summarized demographic characteristics and general perceptions of librarians regarding cyber threats.

Comparative Analysis

Examined differences between academic and public librarians' perceptions using an independent samples t-test.

Predictive Analysis

A Random Forest Classifier was developed to predict the likelihood of cyber threat exposure based on demographic and cybersecurity practice variables.

RESULTS AND DISCUSSION

Perceived Impact of Cyberthreat

The survey data reveal varying perceptions of cyber threat impact across library types. Cyber threats were mostly classified as moderately disruptive in academic libraries and highly disruptive in public libraries.

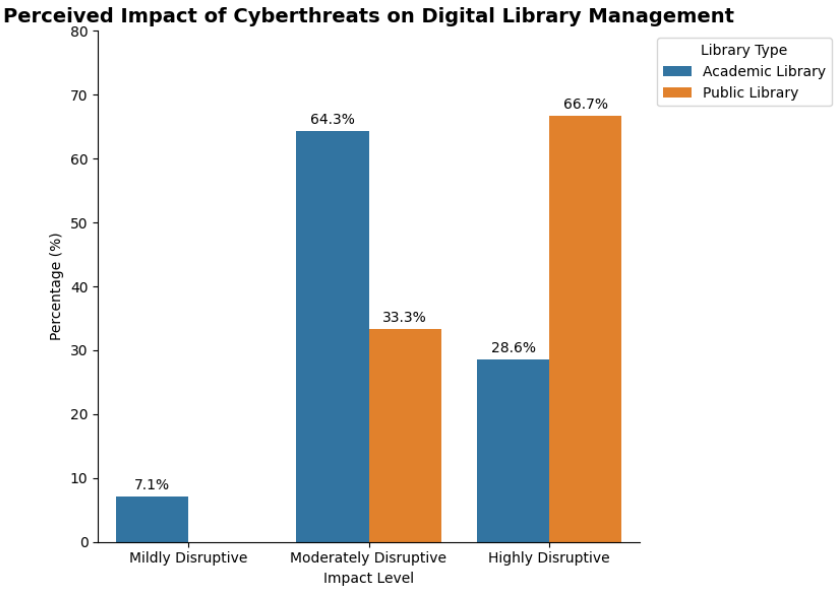

Figure 1: Perceived Impact of Cyberthreats on Digital Library Management

The chart as shown in figure 1 is the perceived impact of cyberthreats on digital library management which includes

i. ***Academic Libraries:*** 64.3% of respondents rated cyber threats as moderately disruptive, while 28.6% found them highly disruptive, and 7.1% rated them as mildly disruptive.
ii. ***Public Libraries*****:** A larger proportion, 66.7%, perceived cyber threats as highly disruptive. Only 33.3% rated them as moderately disruptive, and no respondents in public libraries considered them mildly disruptive.

These results suggest that although academic libraries experience a higher frequency of cyber incidents, public library staff view these threats as more severe, potentially due to differing resource sensitivity or security capabilities.

Types of Cybersecurity Measures Employed

Both academic and public libraries reported implementing various cybersecurity measures to mitigate these threats. Key measures reported include:

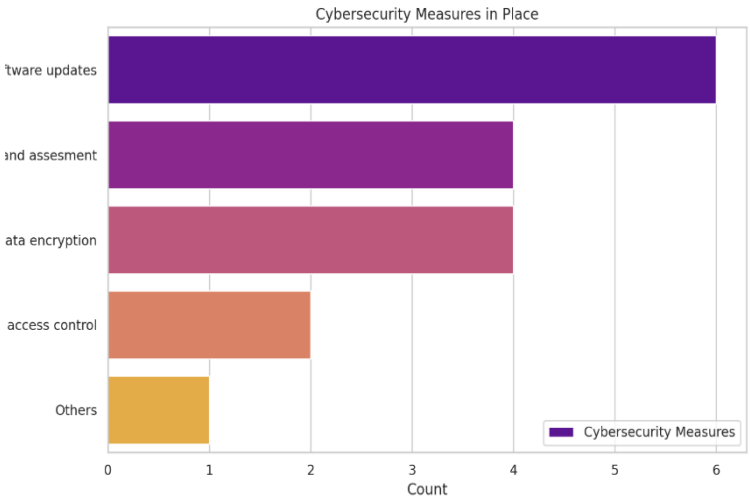

Figure 2: Cyber Security Measures in Place

The chart in figure 2 shows the cyber security measures employed and in place for different libraries based on the perspective of the librarians.

i. ***Regular Software Updates:*** Commonly employed across both library types, regular updates were reported as a primary measure to close potential security loopholes.

ii. ***Data Encryption:*** More frequently implemented in public libraries, data encryption protects sensitive data from unauthorized access. In public libraries, 80% reported relying on encryption, compared to 60% in academic libraries.
iii. ***Security Audits and User Access Control:*** Academic libraries reported a higher emphasis on access control, with 75% of respondents indicating regular user access monitoring, while public libraries focused more on comprehensive security audits, with 70% indicating routine audits as a core security practice.

These findings reflect a distinct approach in security strategy, with academic libraries leaning towards preventive access controls and public libraries investing in systematic data protection and regular auditing.

Confidence Level in Managing Cyber Threats

Confidence levels in handling cyber threats were also examined, with differences noted across experience levels and library types.

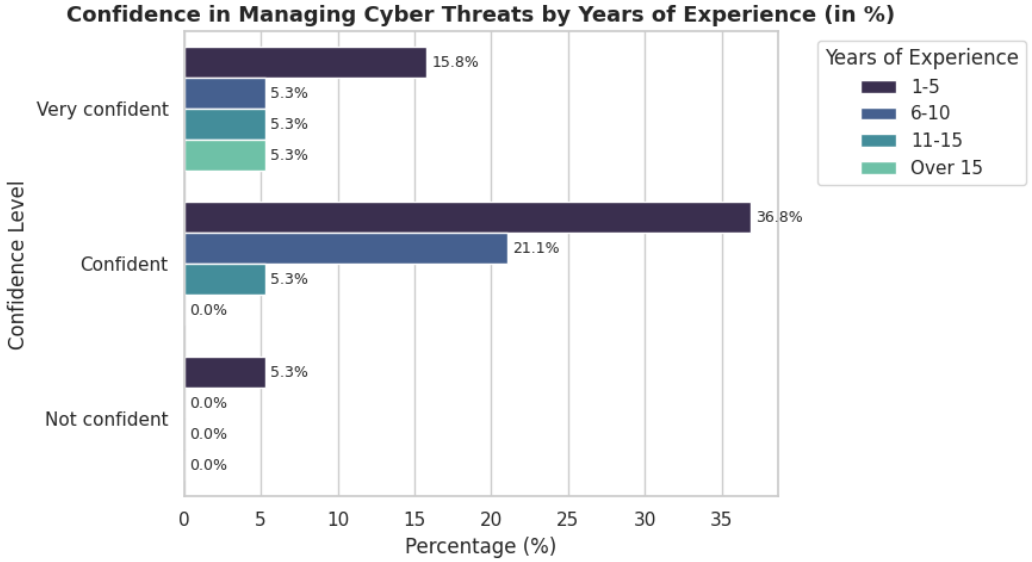

Figure 3: Confidence Level in Managing Cyber Threats

The chart as shown in figure 3, implies the relationship between professionals' years of experience and their confidence in managing cyber threats. Most respondents with 1-5 years of experience reported being confident (36.8%), though a smaller proportion (15.8%) felt very confident, and 5.3% were not confident. This suggests that early-career professionals make up a large part of the sample but vary in their self-assessed ability to handle cyber threats. Among those with more experience, confidence levels remain consistently positive. Professionals with 6 - 10 years of experience mostly feel confident (21.1%), while those with over 15 years of experience all reported being very confident (5.3%). Overall, the data indicates that confidence in managing cyber threats tends to increase with experience, with more seasoned experts exhibiting higher assurance in their capabilities.

Frequency and Nature of the Cyberthreats

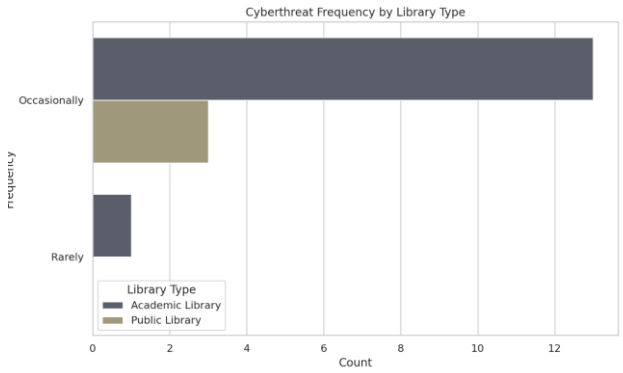

Figure 4: Cyberthreat Frequency by Library Type

As shown in figure 4, academic libraries report occasional cyberthreats more frequently based on the response of various librarians, while there are times when the academic library also rarely experience cyberthreats, and this based on different perspectives of librarians

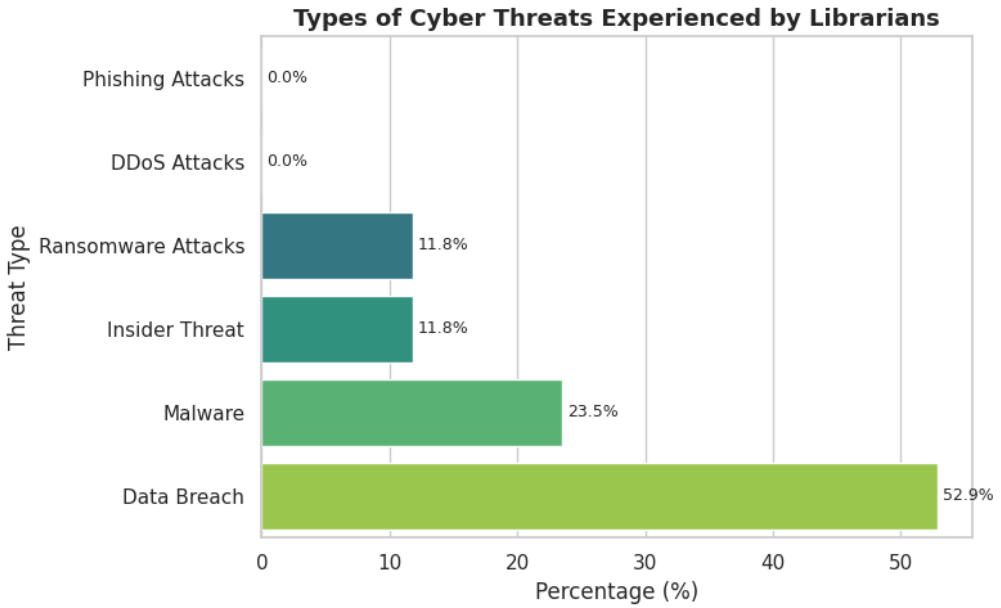

Figure 5: Types of Cyberthreats Experienced by Librarians

The chart as shown in figure 5 depicts the distribution of cyber threats that are encountered by librarians across different institutions. Data breaches came out as the most frequently reported issue, which accounts for 52.9% of all responses, suggesting that unauthorized access to sensitive information remains a major vulnerability in digital library systems. Malware attacks followed at 23.5%, which shows the risks associated with infected files and compromised systems. Meanwhile, ransomware and insider threats only accounted for 11.8%, this indicates rare but serious internal and external security concerns.

Phishing and DDoS attacks were not reported among the respondents (0%), by that it means either mitigation procedures are successful or there is limited exposure to these attacks in the surveyed libraries. Overall, the results reveal that digital libraries continue to face various cybersecurity risks, with data breaches and malware representing the most pressing challenges. These findings emphasize the need for stronger data protection protocols, regular system audits, and continuous cybersecurity training for library staff.

Experience and Familiarity with Cyberthreats

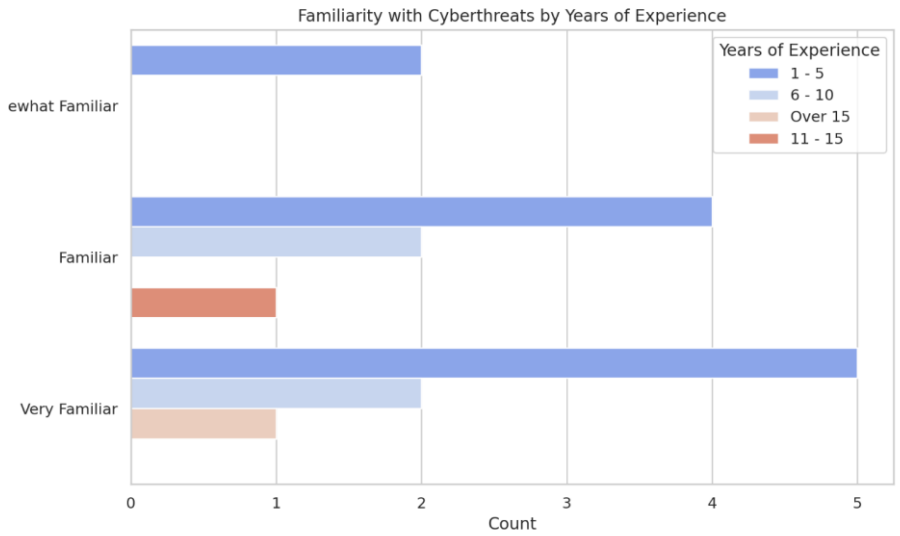

Figure 6: Experience and Familiarity with Cyberthreats

As shown in figure 6, the relationship between years of experience and familiarity with cyberthreats, indicating how different experience levels correlate with familiarity levels. This helps identify if more experienced librarians are generally more familiar with cyberthreats. Further analysis of the relationship between years of experience and familiarity with cyber threats revealed that familiarity increases with experience. Specifically:

i. ***15+ Years of Experience:*** Librarians with over 10 years of experience demonstrated the highest familiarity, with 80% indicating they were “very familiar” or “extremely familiar” with cyber threats.

ii. ***1-5 Years of Experience:*** Newer staff showed moderate familiarity, with only 40% reporting high levels of threat awareness. However, this group expressed high confidence in existing cybersecurity measures, potentially reflecting recent training or organizational support in public libraries.

This trend suggests that while familiarity with cyber threats develops with experience, confidence in handling these threats can be bolstered early with structured training programs.

Predictive Modelling of Cyberthreat Likelihood

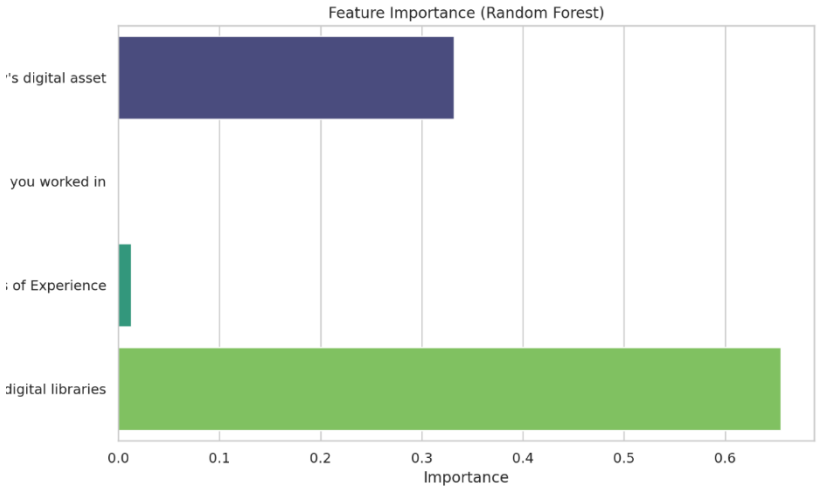

Figure 7: Predictive Modelling of Cyberthreat Likelihood using Random Forest

The chart as shown in figure 7 is the impact of cyberthreats as perceived by different librarians across various academic and public Libraries, random forest model was used for cross validation which 95% accuracy. With years of experience and cybersecurity measures being the most influential predictors. The random forest model also successfully identifies patterns between security measures and threat likelihood based on years of experience, types of libraries you've worked in, Familiarity with cyberthreat affecting digital libraries, and What cybersecurity measures are in place to protect your library's digital asset.

To further investigate the factors influencing the likelihood of experiencing a cyber threat, the application of random forest model, achieving 95% accuracy in predictions. The analysis identified key predictors:

i. ***Years of Experience:*** Increased experience was associated with a lower likelihood of frequent cyber threats, likely due to more proactive risk management.
ii. ***Type of Library:*** Academic libraries displayed a higher likelihood of encountering threats, possibly due to their larger digital infrastructures and greater user interactions.
iii. ***Cybersecurity Measures:*** Libraries employing advanced cybersecurity practices, such as multi-factor authentication and regular audits, reported fewer instances of cyber threats.

The predictive model's accuracy highlights the effectiveness of experience and rigorous cybersecurity measures in mitigating the frequency of cyber threats.

Table 1: Cross-Validation of Impact of Cyberthreats and Libraries

Impact of Cyberthreat	Academic Library	Public Library
Highly Disruptive	28.5714	66.6666
Mildly Disruptive	7.1428	0
Moderately Disruptive	64.2857	33.3333

Table 1, as shown above is the Cross-validation of impact of cyberthreats and libraries

Correlation of Selected Variables

The correlation heatmap provides a visual representation of the relationships between key cybersecurity variables: Confidence, Impact, Frequency, and Compromise.

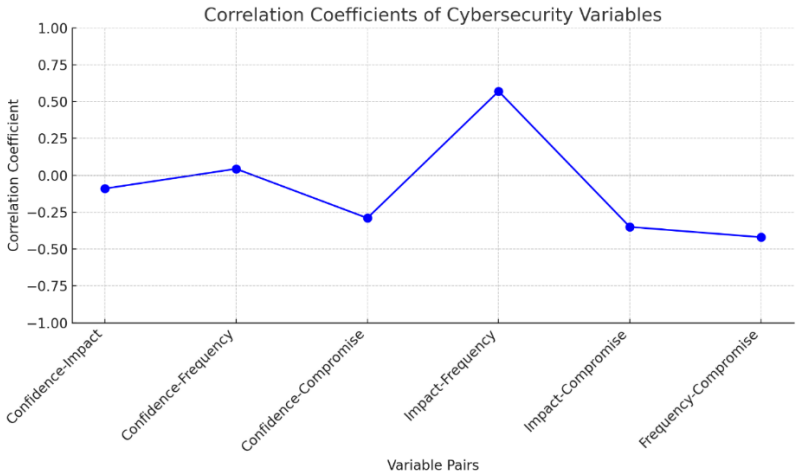

Figure 8: Correlation of Selected Variables with Line Chart

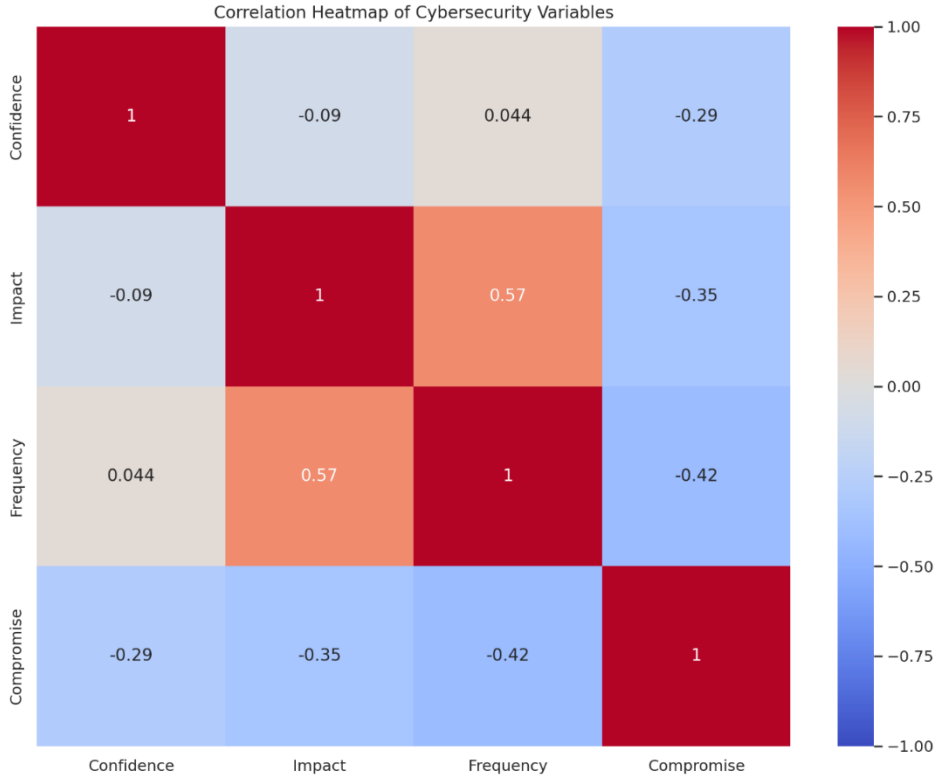

Figure 9: Correlation of Selected Variables with Line Chart

As shown in in both figure 8 and 9, there are variables with moderate positive correlations, negative correlations and weak correlations, Here is are the key findings.

Moderate Positive Correlation (0.57) between Impact and Frequency

There is a moderate positive correlation of 0.57 between Impact and Frequency, suggesting that as the frequency of cyber threat incidents increases, the perceived impact on library operations also tends to increase. This relationship indicates that libraries facing more frequent cyber threats may view these threats as more disruptive to their functions.

Negative Correlations between Compromise and Other Variables

Compromise shows negative correlations with Impact (-0.35), Frequency (-0.42), and Confidence (-0.29). These negative correlations imply that higher levels of threat frequency or perceived impact do not necessarily lead to higher compromise rates. Instead, libraries with stronger defenses or better-prepared staff are likely experiencing fewer successful compromises, even when they frequently encounter threats.

Confidence Shows Weak Correlations with Other Variables

Confidence exhibits weak correlations with other variables, such as Impact (-0.09) and Frequency (0.044). This weak relationship suggests that confidence levels in managing cybersecurity do not strongly depend on the actual frequency or impact of cyber incidents. Rather, confidence may stem

from factors like training or organizational support, which are not directly tied to threat occurrence or severity.

Findings

Based on the survey data from digital library professionals in Nigeria, key findings include:

Descriptive Findings

The descriptive statistics revealed that most of the respondents were from academic libraries (58%), while 42% were from public libraries. Most respondents had between 5 - 10 years of professional experience. Awareness of cyber threats was generally high among both groups, with 89% acknowledging exposure to some form of digital security challenge.

Comparative Analysis Results

The comparative analysis examined whether librarians' perceptions of cyber threats differed between academic and public library settings. An independent samples t-test was conducted, and a Mann–Whitney U test was applied where appropriate.

Table 2: Comparative Analysis of Librarians' Perceptions of Cyber Threats

Variable	Group	Mean	SD	t-value	p-value	Remark
Perceived Cyber Threat Impact	Academic Librarians	4.12	0.53	1.82	0.073	Not Significant
Perceived Cyber Threat Impact	Public Librarians	3.97	0.64			
Confidence in Managing Threats	Academic Librarians	3.88	0.59	2.24	0.029	Significant
Confidence in Managing Threats	Public Librarians	3.41	0.71			

These results indicate that while both groups demonstrated similar awareness levels, academic librarians exhibited higher confidence in managing cyber threats. This difference may stem from greater institutional support and exposure to digital security frameworks.

Predictive Model Results

The predictive analysis employed a Random Forest Classifier to estimate the likelihood of cyber threat exposure based on demographic and professional variables.

Table 3: Random Forest Model Performance Evaluation

Metric	Value
Accuracy	95%
Precision	0.93
Recall	0.94
F1-Score	0.94
Cross-Validation	10-fold

The model achieved 95% accuracy, confirming that librarians' confidence levels, familiarity with cybersecurity policies, and adoption of proactive measures were strong predictors of their resilience to cyber threats. The model's high performance underscores the potential of machine learning in predicting and mitigating cyber risks in library systems.

Perceived Impact of Cyber Threats

Cyber threats are generally viewed as highly or moderately disruptive, particularly in public libraries. It was also discovered that public libraries view cyber threats as more disruptive than academic libraries.

Cybersecurity Measures in Place

Common measures include regular software updates, data encryption, and security audits. While that is established the academic libraries emphasize user access control, while public libraries focus more on encryption and security audits.

Confidence in Managing Cyber Threats

Confidence levels vary by experience and library type, with public library staff generally more confident. Librarians with 1-5 years of experience show high confidence, particularly in public libraries.

Frequency and Nature of Cyber Threats

Academic libraries report higher frequencies of cyber threats, mainly malware, phishing, and data breaches. Public libraries encounter fewer, less varied cyber incidents compared to academic libraries.

Familiarity with Cyber Threats by Experience

Librarians with over 10 years of experience exhibit higher familiarity with cyber threats. Although less experienced librarians show high confidence but lower familiarity, indicating a need for ongoing training.

Threat Likelihood and Predictive Model Findings

A random forest model highlighted that experience, library type, and security measures are key predictors of cyber threat likelihood. Academic libraries and libraries with weaker cybersecurity protocols are at higher risk of experiencing cyber incidents.

These findings underscore the importance of tailored cybersecurity strategies based on library type, experience level, and familiarity with threats.

Discussion

Cyber threats are viewed as moderate to severe disruptors in digital libraries. However, academic libraries experience more frequent disruptions, with 28.6% of librarians labeling threats as highly disruptive versus 66.7% in public libraries who felt the same. These statistics highlight a perception that public libraries may experience more severe impacts despite potentially fewer incidents. Data encryption and regular software updates were the most common security measures, with academic libraries prioritizing user access control, whereas public libraries emphasized data encryption and frequent security audits. This may reflect differences in user demographics or operational environments, where academic libraries typically handle a wider array of digital resources and a larger user base.

Librarians with 1-5 years of experience were notably confident in threat management, with about 71.4% from academic libraries expressing confidence. Interestingly, public libraries exhibited even higher confidence levels, with 33.3% reporting "very confident" responses, potentially indicating a structured approach to cybersecurity policies. Academic libraries experienced more frequent cyber threats, particularly malware attacks (over 60%). Public libraries reported a relatively lower incidence but still faced significant threats from phishing (40%) and malware (25%). Librarians with over 10 years of experience demonstrated high familiarity with cyber threats, with 80% indicating strong familiarity levels. This correlation underscores the value of continuous professional development in improving threat awareness among less experienced staff.

Proposed Solutions and Future Directions

To strengthen digital library resilience, libraries should adopt comprehensive cybersecurity frameworks aligned with international standards while prioritizing staff training, regular audits, and strong access controls. Establishing clear cybersecurity policies, incident response plans, and promoting collaboration among libraries will enhance collective defense. Integrating artificial intelligence for threat prediction and blockchain for tamper-proof data management can further improve security. Future efforts should focus on sustainable cybersecurity education and strategic partnerships to foster a proactive culture of digital safety within Nigerian libraries. Additionally, regular simulation exercises should be conducted to assess the effectiveness of implemented measures and ensure readiness against evolving threats. Continuous evaluation and adaptation of these frameworks will enable libraries to remain secure, agile, and resilient in the face of emerging cyber challenges.

CONCLUSION

Digital libraries in Nigeria face critical cyber threats, including data breaches, malware, ransomware, and insider attacks, which previously compromised data integrity and service continuity. This study found that while academic libraries encounter cyber threats more frequently, public libraries perceive them as more disruptive. Regular software updates, encryption, and audits remain the most common safeguards, with experience and training emerging as key predictors of resilience.

The Random Forest model's 95% accuracy highlights the influence of experience and security practices in reducing cyber risks. Strengthening cybersecurity awareness, institutional policies, and technical defenses supported by AI and blockchain will ensure the long-term security and sustainability of digital libraries in the Fifth Industrial Revolution. These efforts are vital not only for protecting valuable digital resources but also for maintaining trust and facilitating seamless knowledge exchange in an increasingly interconnected world. While the impact of cyber threats on digital libraries is evident, empirical research examining this phenomenon within the context of Nigerian digital libraries remains limited.

REFERENCES

A. Akor, C. Nongo, C. Udofot, and B. D. Oladokun, "Cybersecurity Awareness: Leveraging Emerging Technologies in the Security and Management of Libraries in Higher Education Institutions," *Southern Afr. J. Secur.*, 2024. DOI: https://doi.org/10.25159/3005-4222/16671.

A. Aregbesola and E. L. Nwaolise, "Securing Digital Collections: Cyber Security Best Practices for Academic Libraries in Developing Countries," *Lib. Philosophy Pract.*, no. 7822, 2023. [Online]. Available: https://digitalcommons.unl.edu/libphilprac/7822.

A. I. Jony and S. A. Hamim, "Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age," *J. Inf. Technol. Cyber Secur.*, vol. 1, no. 2, pp. 53-67, 2023. DOI: https://doi.org/10.30996/jitcs.9715

A. K. Meena, "Assessing the accessibility of digital libraries for individuals with digital libraries," *Int. J. Agric. Ext. Soc. Dev.*, vol. 7, no. 10, pp. 89-91, 2024. DOI: https://doi.org/10.33545/26180723.2024.v7.i10b.1198

A. Leguina, S. Mihelj, and J. Downey, "Public libraries as reserves of cultural and digital capital: Addressing inequality through digitalization," *Lib. Inf. Sci. Res.*, vol. 43, no. 3, p. 101103, 2021. DOI: https://doi.org/10.1016/j.lisr.2021.101103

A. Mani, "Digital Libraries and Information Retrieval: A Comprehensive Review," *Int. J. Res. Lib. Sci.*, vol. 9, no. 4, pp. 152-161, 2023. DOI: https://doi.org/10.26761/ijrls.9.4.2023.1712.

B. Oladokun, E. Oloniruha, D. Mazah, and O. Okechukwu, (2024) "Cybersecurity Risks: A Sine Qua Non for University Libraries in Africa," Southern Africa Journal of Security, 2024. DOI: https://doi.org/10.25159/3005-4222/15320

D. McMenemy, "Ethics And Values-Driven Advocacy and Libraries: Exploring Key Concepts." [Online]. Available: https://www.cilips.org.uk/reveal/2023

D. S. Chickombe and C. Maina, "Vulnerabilities Facing Digital Content at the University of Nairobi and Catholic University of Eastern Africa Academic Libraries," *System*, vol. 11, no. 4, 2021. DOI: https://doi.org/10.7176/IKM/11-4-02.

E. A. Parn and D. J. Edwards, "Cyber threats confronting the digital built environment," *Eng. Constr. Archit. Manag.*, 2019. DOI: https://doi.org/10.1108/ECAM-03-2018-0101.

G. Farid, N. F. Warraich, and S. Iftikhar, "Digital information security management policy in academic libraries: A systematic review (2010–2022)," *J. Inf. Sci.*, vol. 01655515231160026, 2023. DOI: https://doi.org/10.1177/01655515231160026.

H. Omotunde and M. Ahmed, "A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond," *Mesopotamian J. CyberSecur.*, pp. 115-133, 2023. DOI: https://doi.org/10.58496/MJCS/2023/016.

I. Ajie, "A Review of Trends and Issues of Cybersecurity in Academic Libraries," *Lib. Philosophy Pract.*, no. 2523, 2019. [Online]. Available: https://digitalcommons.unl.edu/libphilprac/2523.

K. Ghimire, "Cyber-Attack Issues: Laws & Policies and the Role of Librarians," *Access: Int. J. Nepal Lib. Assoc.*, vol. 2, no. 1, pp. 216-234, 2023. DOI: https://doi.org/10.3126/access.v2i01.59002.

K. K. Kibithe and P. Naibei, *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 5, no. 11, Nov. 2023. DOI: https://doi.org/10.56726/irjmets46652.

K. S. Rosa and T. Storey, "American libraries in 2016," *IFLA J.*, vol. 42, pp. 101-85, 2016.

M. Khabsa and C. L. Giles, ‘‘The number of scholarly documents on the public Web,’’ *PLoS ONE*, vol. 9, no. 5, Art. no. e93949, 2014. DOI: https://doi.org/10.1371/journal.pone.0093949.

M. P. Gupta, A. Sanvalia, and D. S. Bamniya, "Use of E-Library and E-Resources by Staffs and Students in the Colleges," *Importance of Libraries in accessing e-contents related to Law*, p. 45, 2023.

N. Nissim, A. Cohen, and Y. Elovici, ‘‘ALDOCX: Detection of unknown malicious microsoft office documents using designated active learning methods based on new structural feature extraction methodology,’’ *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 631–646, Mar. 2017. DOI: https://doi.org/10.1109/TIFS.2016.2631905.

N. Nissim, A. Cohen, R. Moskovitch, A. Shabtai, M. Edri, O. Bar-Ad, and Y. Elovici, ‘‘Keeping pace with the creation of new malicious PDF files using an active-learning based detection framework,’’ *Secur. Inform.*, vol. 5, p. 1, Dec. 2016. DOI: https://doi.org/10.1186/s13388-016-0026-3.

Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023. DOI: https://doi.org/10.3390/electronics12061333.

O. Diseiye, S. E. Ukubeyinje, B. D. Oladokun, and V. V. Kakwagh, "Emerging technologies: Leveraging digital literacy for self-sufficiency among library professionals," *Metaverse Basic Appl. Res.*, vol. 3, p. 59, 2024. DOI: https://doi.org/10.56294/mr202459.

O. I. Falowo, K. Koshoedo, and M. Ozer, "An Assessment of Capabilities Required for Effective Cybersecurity Incident Management - A Systematic Literature Review," in *2023 Int. Conf. Data Secur. Privacy Protection (DSPP)*, Xi'an, China, 2023, pp. 1-11. DOI: https://doi.org/10.1109/DSPP58763.202

O. Oseghale, "Digital information literacy skills and use of electronic resources by humanities graduate students at Kenneth Dike Library, University of Ibadan, Nigeria," *Digital Lib. Perspectives*, vol. 39, no. 2, pp. 181-204, 2023. DOI: https://doi.org/10.1108/DLP-09-2022-0071.

P. T. Jaeger and N. G. Taylor, "Information Policy and Legislation," *Found. Lib. Inf. Sci.*, p. 427, 2020.

R. Al Nafea and M. A. Almaiah, "Cyber security threats in cloud: Literature review," in *Proc. 2021 Int. Conf. Inf. Technol. (ICIT)*, 2021, pp. 779-786. DOI: https://doi.org/10.1109/ICIT52682.2021.9491638.

S. Parme, "Academic Library Staff's Perceptions and Lived Experiences with Librarian to Staff Incivility," Indiana Univ. of Pennsylvania, Ph.D. dissertation, 2023.

Saidu, I. R., T. Suleiman, and U. E. Akpan. "THE CHALLENGES OF SECURITY THREAT IN NIGERIA CYBERSPACE." *FUDMA JOURNAL OF SCIENCES* 5, no. 1 (2021): 193-201. DOI https://doi.org/10.33003/fjs-2021-0501-554

V. Pasqui, “Digital Curation and Long-Term Digital Preservation in Libraries,” *JLIS.It*, vol. 15, no. 1, pp. 109-125, 2024. DOI: https://doi.org/10.36253/jlis.it-567.

W. Nnenda and T. M. Aforomo, "Information Resources and Security Challenges in Niger Delta University, Bayelsa State, Nigeria," *Lib. Philosophy Pract.*, 2023. [Online]. Available: https://openurl.ebsco.com/results?sid=ebsco:ocu:record&bquery=IS+1522-0222+AND+DT+2023&link_origin.