C
J
L
I
L

THE CATALYST JOURNAL OF LIBRARY AND INFORMATION LITERACY

Vol 4(2), December, 2025 ISSN:2971-7094

“https://journals.journalsplace.org/index.php/CJLIL

PREPAREDNESS AND RESPONSE PRACTICES OF LIBRARIANS ON CYBERSECURITY INCIDENCES IN DIGITAL INFORMATION SERVICE DELIVERY IN UNIVERSITY LIBRARIES IN KATSINA STATE, NIGERIA

by

Safiyya Kabir Ifo
Department of Library & Information Science,
Umaru Musa Yar’adua University Katsina

Dr. Lawal Umar
Department of Library & Information Science,
Umaru Musa Yar’adua University Katsina
lawal.umar@umyu.edu.ng
Corresponding Author
&
Dr. Muhammad Kabir Abubakar
Department of Library & Information Science,
Umaru Musa Yar’adua University Katsina

Abstract

The study investigated preparedness and response practices of librarians on cybersecurity incidences in digital information services delivery in university libraries in Katsina State, Nigeria. Three (3) research questions guided the study. These questions included what types of cybersecurity incidence are experienced in digital information service delivery by university libraries in Katsina state? What are the preparatory mechanisms adopted to prevent cybersecurity incidence in digital information service delivery in university libraries in Katsina State? What are the response practices adopted to mitigate cybersecurity incidence in digital information service delivery by university libraries in Katsina state? The study employed descriptive survey design and the population of the study comprised of all the One Hundred and Six (106) librarians in all the four (4) university libraries in Katsina State. Total enumeration sampling technique was used to select all the 106 librarians as the sample size for the study. Questionnaire was the instrument used for data collection and was validated by experts in the fields and reliability result was .872. The data was analyzed using simple frequency Tables, Percentages, Means and Standard deviation. The findings showed that university libraries in Katsina State face widespread cybersecurity issues, primarily unauthorized access and network failures. Additionally, the study found that although some preparatory measures, such as digital resource management planning and software updates, have been initiated, key areas like firewall protection, staff training and vulnerability assessments are still lacking highlighting the urgent need for targeted training and strategic support to enhance digital service delivery and security across these libraries. It was concluded that while university libraries in Katsina State have provided some foundational cybersecurity protocols, their overall preparedness and response capabilities remain insufficient to address the evolving landscape of digital threats. The study recommended that University libraries in Katsina State should strengthen their cybersecurity monitoring systems to prevent common issues like unauthorized access and network failures, improve the adoption of cybersecurity preventive measures, particularly strengthening password policies, increasing user education on cybersecurity best practices and among others.

Keywords*: C*ybersecurity Incidence, Cybersecurity Preparedness, Response Practices, Digital Information Service Delivery

Introduction

University libraries serve as information hubs, providing digital information resources and services to support teaching, learning, and research. Traditionally, libraries relied on physical materials such as books and journals, with access limited by the library's physical space and operating hours (Ryder &Madhavan, 2019). Advancements in digital technology have transformed university libraries, enabling remote access to electronic resources like e-books, e-journals, and databases, while tools such as online catalogues, digital repositories, and virtual reference services enhance search efficiency and support academic needs. These transformations have significantly expanded accessibility and convenience of library services for students, faculty, and researchers. Conversely, it has also presented challenges related to copyright, user data privacy, and digital preservation, which library staff and administrators must actively address (George & Onyema, 2020).

In today's world, cybersecurity has now become a global concern. Protecting personal data on the Internet is a major concern, with the number of connected devices surpassing 50 billion as at 2020 (Yusuf et al, 2021). Cybersecurity are measures taken to protect computer systems, resources, users, and information against unauthorized access and attacks. Cybersecurity are also techniques generally set forth in published materials that attempt to safeguard the cyber environment of user or organization, maintaining the integrity of networks, programs, and data. Cyber incidents including natural disasters, human errors, and software vulnerabilities like viruses and hacking pose serious threats to digital information systems in university libraries, leading to data loss, service disruptions, and privacy breaches (Luft, 2020).

In Nigeria, common cybercrimes that have been reported in libraries include unauthorized access, identity theft, and malware attacks (Muhammad et al, 2020). Similarly, university libraries in Katsina State are not free from these cybercrimes. To address these threats, robust preparatory mechanisms such as planning, detection, response, and recovery are essential. Equipping librarians with cybersecurity knowledge and tools is crucial for effective threat management. Musa and Maifata (2020) emphasized that response practices, including security protocol implementation, regular software updates, audits, and user education are vital for protecting digital information services in university libraries. Preparatory mechanisms for preventing cybersecurity incidents in digital information service delivery involve a blend of technical, administrative, and procedural measures aimed at minimizing vulnerabilities and protecting sensitive data. These measures are essential for safeguarding against potential cyber threats and include proactive planning, policy implementation, and regular system assessments (Pathak, 2019; Masenya & Chisita, 2022). Response practices, as noted by Alzyadi et al (2021), help organizations manage incidents effectively, mitigate damage, and enhance their overall cybersecurity posture through continuous learning and strategic improvement.

This study therefore, aims to investigate the preparedness and response practices of librarians on cybersecurity incidences adopted in digital information services delivery in university libraries in Katsina State, Nigeria.

Statement of the Problem

In this digital age, university libraries must prioritize cybersecurity to ensure safe and uninterrupted access to digital information services, as growing technological dependence exposes them to various threats and vulnerabilities. Studies such as Musa and Maifata (2020); Nikhat, et al (2021) reported high rate of cybersecurity incidents, such as data breaches and service interruptions, particularly in Nigeria's National Communication Commission, which similarly affect libraries and hinder their core functions. Despite the recognized importance of cybersecurity incidents preparedness and response practices for managing such threats, empirical evidence suggests that technical, administrative, and procedural measures for preventing and responding to cyber incidents are lacking in university libraries in Katsina State. Moreover, there is a scarcity of empirical research in library and information science focusing on cybersecurity incidents and response strategies. Consequently, the study investigated the preparedness and response practices of librarians on cybersecurity incidences in digital information service delivery in university libraries in Katsina State, Nigeria.

Research Questions

The following research questions were formulated to guide the study:

1. What types of cybersecurity incidence are experienced in digital information service delivery by university libraries of in Katsina state
2. What are the preparatory mechanisms adopted to prevent cybersecurity incidence in digital information service delivery in university libraries in Katsina State?
3. What are the response practices adopted to mitigate cybersecurity incidence in digital information service delivery by university libraries in Katsina state?

Literature Review

Relevant literatures were reviewed in line with the research questions raised for the study as follows:

Types of cybersecurity incidences on digital information service delivery in university libraries

There are so many cybersecurity incidences on digital information service delivery which include data breaches, malware attacks, phishing attacks, Denial of Service (DoS) attacks, unauthorised access, insider attacks and social engineering attacks among others. According to Huang, et al (2019), Ngulube (2019), the types of cybersecurity incidences face by university libraries includes computer virus, hacking, unauthorized access to information resources, corrupting data, or gaining access to programs and confidential information, password sniffing, impersonation, viruses, Trojans, adware and spyware, ransomware attack on the information system, stealing of user‟s bio data from the library system, website spoofing, cyber extortion, Interception of electronic message, and Denial of service attacks. In the context of university libraries, cybersecurity incidences as identified by Ajie (2019), Ibrahim & Umar (2020), include; Hardware security threats such as natural disasters; earthquakes, fires, floods and thunder strokes; changes in temperature or humidity; accidents, such as stealing and vandalism etc; Software Security Threats, Network Security Threats, destruction of information and other resources, corruption or modification of information, theft, removal or loss of information and human related threats respectively.

These types of cybersecurity incidences can jeopardize the integrity and confidentiality of information resources towards effective and efficient services delivery in the university libraries. Also, in African countries such as Nigeria, South Africa, Angola, Morocco, Algeria, Tunisia, Egypt, Libya, and Sudan Museba, et al (2021) revealed that networked computer systems are exposed to unprecedented vulnerabilities and they have considerably affected various sectors on the African continent such as education, trade and commerce, manufacturing and production, banking and finance, agriculture, and public service. In Nigeria Okike and Adetoro (2019) revealed that librarians had witnessed threats on their information systems. Malware was the major threat to the database/OPAC system similarly Malware (Virus and Worms) is the major threat to the operating systems across the universities libraries.

Preparatory mechanisms adopted to prevent cybersecurity incidences

Preparatory mechanisms to prevent cybersecurity incidents in digital information service delivery involve a mix of technical, administrative, and procedural measures aimed at reducing vulnerabilities and safeguarding sensitive data. According to Pathak (2019) and Masenya and Chisita (2022), these measures include implementing robust security infrastructure, performing regular software updates, securing access controls, conducting vulnerability assessments and penetration testing, providing cybersecurity awareness training, and establishing incident response plans. By adopting these proactive measures, organizations can reduce vulnerabilities and enhance their overall cybersecurity posture, thereby minimizing the likelihood of cyberattacks and protecting sensitive data. In the context of university libraries, preparatory mechanisms adopted to prevent cybersecurity incidents in digital information service delivery involve a series of proactive measures aimed at safeguarding sensitive data and maintaining (Yusof & Saman, 2016; Yusuf, et al, 2022).

In developing countries, like Malaysia studies such as (Akor, et al) found that librarians employ several preparatory mechanisms to prevent cybersecurity incidents. This involves educating library staff about cybersecurity best practices and raising awareness about common threats like phishing attacks and malware. Hussain and Ahmad (2021) prioritized the implementation of robust cybersecurity measures, such as firewalls, encryption, and intrusion detection systems, to protect sensitive patron data from unauthorized access and cyber threats. Additionally, librarians collaborate with government agencies, cybersecurity experts, and other libraries to share information, resources, and strategies to enhance their cybersecurity posture and safeguard the integrity and confidentiality of library resources and patron information.

Response practices adopted to mitigate cybersecurity incidences in digital information services delivery by university libraries

Response practices to mitigate cybersecurity incidents consist of a series of actions organizations take to effectively address and manage cyber threats and breaches. Alzyadi, et al (2021) highlight that these practices help organizations reduce damage, improve security, and learn from past incidents to enhance strategies. Ershova, et al (2021) further explained that an effective response involves developing and implementing a comprehensive incident response plan, which includes preparation, detection, containment, eradication, recovery, and post-incident review to continuously improve security measures and response efforts. Key components include preparation and planning, detection and identification of incidents, containment and isolation, eradication of threats, recovery and restoration of systems, and conducting post-incident reviews to continuously refine security measures and response strategies. University libraries employ various response practices to mitigate cybersecurity incidents in digital information service delivery.

Theoretical framework

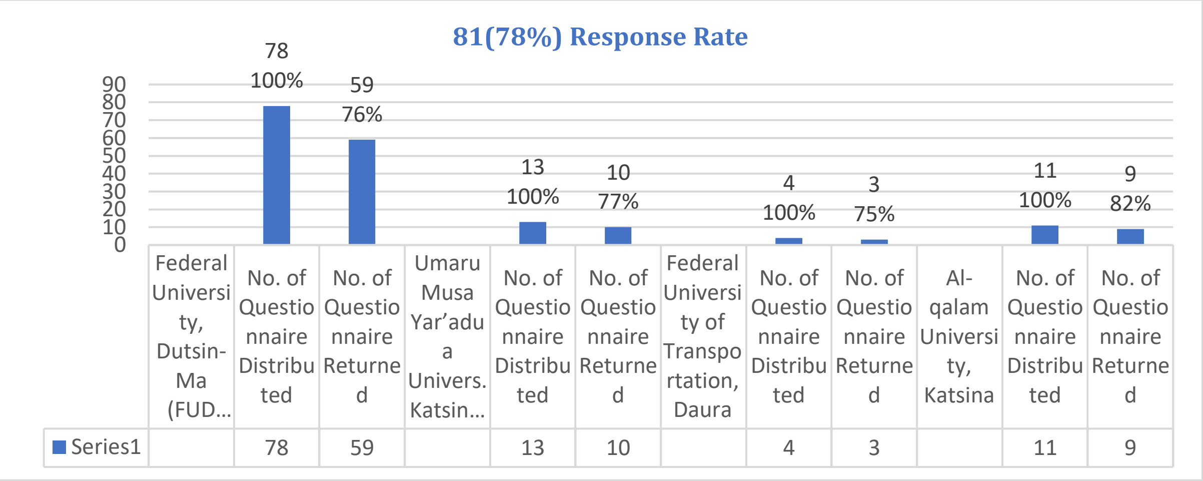
The study was guided by Cybersecurity Capability Maturity Model (C2M2) developed by the US Department of Energy and first published in 2012. This model provides a framework for organizations to assess and improve their cybersecurity capabilities. There is also the National Institute of Standards and Technology Cybersecurity Framework (NIST CF), which provides guidelines for organizations to identify, protect, detect, respond, and recover from cyber security incidents. And lastly, the study will be guided based on Cybersecurity Capability Maturity Model (C2M2). The model focuses on ten domains, (Daltas & Gudgel, 2020), by focusing on the ten domains, organizations will be able to develop strategies for continuous improvement, ultimately leading to more robust protection against cyber threats. Several studies have applied the Cybersecurity Capability Maturity Model (C2M2) to assess and improve cybersecurity capabilities in various sectors. For examples, Sust and Vancza (2017) assess the cybersecurity capabilities of small businesses. The authors found that small businesses often lack formal cybersecurity programs and have low maturity levels in domains such as Risk Management and Incident Management. They emphasized the need for small businesses to prioritize cybersecurity investments and utilize models like C2M2 to enhance their security posture.

Methodology

The study employed descriptive survey design and the population of the study comprised of all librarians that hold first degree in library and information science in all the four (4) universities in Katsina state, which is one hundred and six (106). Total enumeration sampling technique was used where all the 106 librarians were selected as the sample size for the study. A self-developed questionnaire was the instrument used for data collection and was validated using face and content validity by experts in the fields of library and information science. To make sure that the instrument is reliable, 40 copies of the questionnaire were distributed to similar group of respondents in two universities including Bayero University Kano and Maitama Sule University Kano who were not part of the study for inter-item internal consistency reliability. This was carried out before the actual distribution of the questionnaire. Cronbach Alpha Coefficient was used to test the reliability result and was .872. The data was analysed using descriptive statistics where simple frequency Tables, Percentages, Means and Standard deviation were used.

Results

A total of one hundred and six (106) copies of questionnaire were distributed to the respondents in the four (4) universities under study and eighty-one (81) copies of questionnaires were duly completed and returned as shown in figure 1.



What types of cybersecurity incidence are experienced in digital information service delivery in your university library?

The respondents were asked to share their opinions on the types of cybersecurity incidents experienced in digital information service delivery within the study area. Table 1 presents these responses, including the corresponding mean scores and standard deviations.

Table 1: Types of cybersecurity incidence experienced in digital information service delivery in the university libraries in Katsina State (N=81):

Types of Cybersecurity Incidence	Yes		No	
	F	**%**	**F**	**%**
Software Piracy: Installing unlicensed software on library computers	23	28.4	58	71.6
Unauthorized account access	60	74.1	21	25.9
Misinformation sharing or disseminating false or misleading information during research assistance	36	44.4	45	55.6
Phishing attacks	26	32.1	55	67.9
Computer viruses	48	59.3	33	40.7
Plagiarism	35	43.2	46	56.8
Intellectual property theft	29	35.8	52	64.2
Cyberbullying such as engaging in or facilitating hate speech or bullying on social media	26	32.1	55	67.9
Legal violations such as inadvertently violating copyright laws	48	59.3	33	40.7
Resource misuse like using library printers or scanners for personal projects without permission	35	43.2	46	56.8
Poor online conduct such as not maintaining professionalism in online interactions	26	32.1	55	67.9
Neglecting cyber hygiene like failing to update software or apply security patches, exposing the library's systems to vulnerabilities	33	40.7	48	59.3
Weak password practices	21	25.9	60	74.1
Social media misconduct	26	32.1	55	67.9
Denial of Service DoS Attacks	33	40.7	48	59.3
Hacking	26	32.1	55	67.9
Power failure	36	44.4	45	55.6
Network failure	60	74.1	21	25.9
System malfunction	55	67.9	26	32.1
Staff incompetence	36	44.4	45	55.6

Based on the data in Table 1, university libraries in Katsina State face various cybersecurity incidents, with unauthorized account access and network failure each reported by 74.1% of respondents, and system malfunction by 67.9%, indicating significant technical and access control vulnerabilities. Other major concerns include computer viruses and copyright infringement (both at 59.3%), highlighting gaps in digital security and legal compliance awareness. Human-related risks such as misinformation sharing (44.4%), staff incompetence (44.4%), and plagiarism (43.2%) also threaten service integrity. Less frequent but notable incidents like phishing, cyberbullying, social media misconduct, and hacking (each at 32.1%) reveal challenges from external threats and behavioural issues. Weak password practices (25.9%) and software piracy (28.4%) were least reported, possibly due to underreporting or insufficient monitoring. Collectively, it exposes systemic weaknesses in cybersecurity preparedness, staff training, and infrastructure, emphasizing the need for comprehensive improvements across technical and operational domains.

What are the preparatory mechanisms adopted to prevent cybersecurity incidence in digital information service delivery in your university library?

The respondents were asked to indicate their opinions on the preparatory mechanisms adopted to prevent cybersecurity incidence in digital information service delivery in the study area. Table 2 shows the responses along with the mean scores and standard deviations.

Table 2: Mean results of preparatory mechanisms adopted to prevent cybersecurity incidence in digital information service delivery (N=81):

Statements	**SD**		**D**		**UD**		**A**		**SA**		**Mean**	**STD**
	F	**%**	**F**	**%**	**F**	**%**	**F**	**%**	**F**	**%**		
The library has created a digital resource management plan for managing and safeguarding digital resources, including access control and usage tracking	12	14.8	23	28.4	0	0	35	43.2	11	13.6	3.12	1.36
The library implemented a robust security infrastructures	11	13.6	35	43.2	0	0	24	29.6	11	13.6	2.86	1.35
The library has set up an advanced security systems like firewalls, IDS, and IPS to protect digital resources	22	27.2	24	29.6	12	14.8	23	28.4	0	0	2.44	1.17
The library creates a detailed policy outlining security protocols, data protection measures, and user responsibilities	22	27.2	35	43.2	0	0	24	29.6	0	0	2.32	1.17
The library ensuring regular software updates like k keeping software applications and operating systems updated to fix vulnerabilities	22	27.2	12	14.8	12	14.8	24	29.6	11	13.6	2.87	1.44
The library secure access control mechanisms by employing multi-factor authentication and role-based access controls to limit access to sensitive information.	11	13.6	23	28.4	12	14.8	35	43.2	0	0	2.88	1.12
The library foster collaboration with IT experts to ensure that library systems are continuously monitored and evaluated for security	19	23.5	24	29.6	24	29.6	23	28.4	4	4.9	2.78	1.23

The library conducted periodic vulnerability assessments to proactively enhance security.	23	28.4	36	44.4	0	0	27	27.2	0	0	2.10	1.24
The library enforced strong password policies to prevent unauthorized access.	35	43.2	11	13.6	12	14.8	11	13.6	12	14.8	2.43	1.52
The library set up user education on cybersecurity best practices about safe online behavior and recognizing threats.	23	28.4	35	43.2	0	0	11	13.6	12	14.8	2.43	1.41
The library ensure auditing and logging system activity to monitor system activities and detect suspicious behavior.	16	19.8	8	9.9	32	39.5	18	22.2	7	8.6	2.90	1.21
The library ensure training and retraining of library staff	19	23.5	24	29.6	24	29.6	23	28.4	4	4.9	2.78	1.23
The library ensure deployment of quality digital information systems resources and facilities	22	27.2	24	29.6	12	14.8	23	28.4	0	0	2.44	1.17
The library ensure employment of competent and qualified library staff	24	29.6	11	13.6	24	29.6	11	13.6	11	13.6	2.68	1.39

Key: SD: Strongly Disagree 1 **D:** Disagree 2 **UD:** Undecided 3 **A:** Agree 4 **SA:** Strongly Agree 5

The data in Table 2 reveal that while university libraries in Katsina State have taken some steps to enhance the security of their digital information services, the implementation of these preparatory mechanisms remains inconsistent and, in many areas, inadequate. The most commonly adopted measure is the development of a digital resource management plan (M = 3.12, SD = 1.36), followed by moderate efforts in software updates (M = 2.87), access control (M = 2.88), and collaboration with IT experts (M = 2.78). However, the average scores suggest these practices are not fully or consistently implemented. More critically, essential technical safeguards like firewalls and intrusion detection/prevention systems are poorly adopted (M = 2.44), and key practices such as vulnerability assessments (M = 2.10), strong password enforcement (M = 2.43), and user cybersecurity education (M = 2.43) are significantly lacking. Low scores in staff training (M = 2.78) and hiring qualified personnel (M = 2.68) further underscore weaknesses in human resource development. The findings highlight a low approach to cybersecurity preparedness, with major gaps in both technological infrastructure and staff capacity that hinder effective risk mitigation in digital library environments.

What are the response practices adopted to mitigate cybersecurity incidence in digital information service delivery by the university library?

The respondents were asked to indicate their opinions on the response practices adopted to mitigate cybersecurity incidence in digital information service delivery in the study area. Table 8 shows the responses along with the mean scores and standard deviations.

Table 3: Mean results of response practices adopted to mitigate cybersecurity incidence in digital information service delivery in the university library (N=81):

Statements	SD		D		UD		A		SA		Mean	STD
	F	**%**	**F**	**%**	**F**	**%**	**F**	**%**	**F**	**%**		
The library ensures regular review of copyright laws and ensures that all digital resource usage complies with legal standards	22	27.2	24	29.6	12	14.8	23	28.4	11	13.6	2.98	1.30
The library provides early warning and early response training for staff on cybersecurity best practices, digital literacy, and emerging threats.	22	27.2	25	30.9	11	13.6	23	28.4	0	0	2.44	1.17
The library ensures regular assessing potential risks to digital services and identifies vulnerabilities within the library's systems.	22	27.2	35	43.2	0	**0**	24	29.6	0	0	2.32	1.17
The library is establishing role-based access controls to limit access to sensitive information and systems based on user needs	11	13.6	35	43.2	0	0	35	43.2	0	0	2.72	1.16
The library prepare clear plans outlining steps to take in the event of a cybersecurity incident, including communication protocols and recovery procedures	11	13.6	24	29.6	11	13.6	24	29.6	11	13.6	3.00	1.30
The library ensures encrypting sensitive data both in transit and at rest to protect against breaches.	11	13.6	37	45.7	10	12.3	12	14.8	11	13.6	2.72	1.27
The library set-up regular backups and disaster recovery plans to ensure data availability and recovery in case of attacks.	22	27.2	24	29.6	12	14.8	12	14.8	11	13.6	2.58	1.39

Key: SD: Strongly Disagree 1 **D:** Disagree 2 **UD:** Undecided 3 **A:** Agree 4 **SA:** Strongly Agree 5

The data in Table 3 indicated that university libraries in Katsina State have adopted some response practices to manage cybersecurity incidents, but overall preparedness remains limited and uneven. The most established measures include the development of incident response plans (M = 3.00, SD = 1.30) and regular reviews of copyright compliance (M = 2.98, SD = 1.30), reflecting a basic awareness of legal and procedural responsibilities. However, technical safeguards such as data encryption and role-based access controls (both M = 2.72) are only moderately implemented, with significant variation in responses. More concerning are the low levels of proactive measures, including regular risk assessments (M = 2.32), staff training for early warning and response (M = 2.44), and disaster recovery practices like regular backups (M = 2.58), all of which are critical to minimizing damage during cybersecurity incidents. These findings indicate that while foundational protocols exist in some libraries, there are substantial gaps in technical infrastructure, staff readiness, and operational planning, limiting the effectiveness of their overall cybersecurity response.

Discussion of findings

1. University libraries in Katsina State face widespread cybersecurity issues, primarily unauthorized access and network failures. These incidents reveal critical vulnerabilities in technical infrastructure and staff training. Consistently, Huang et al. (2019) and Ngulube (2019) found that university libraries globally face pervasive cybersecurity threats like data breaches, malware, and phishing that disrupt digital services. In developed regions, issues include unauthorized access and data manipulation (Peter, 2017; Mandlenkosi & Witness, 2022), while libraries in developing nations report identity theft, email scams, and infrastructure issues (Chingoriwo, 2022; Khalipi, 2023). These incidents universally compromise the integrity and confidentiality of library resources and services, leading to loss of user trust and reduced effectiveness of digital service delivery.
2. University libraries in Katsina State have taken some initial steps towards cybersecurity, such as the development of a digital resource management plan followed by moderate efforts in software updates, access control, and collaboration with IT experts, but these are insufficient. Critical areas like firewalls, staff training, and vulnerability assessments are severely lacking. Similarly, findings by Pathak, (2019) and Masenya and Chisita (2022) revealed that preparatory cybersecurity mechanisms use a blend of technical, administrative, and procedural measures to reduce vulnerabilities and safeguard data. Key strategies include implementing robust security infrastructure, access controls, staff training, and incident response plans. These proactive steps help organizations strengthen their security posture and reduce the risk of cyber-attacks.
3. University libraries in Katsina State have basic incident response plans, such as the development of incident response plans and regular reviews of copyright compliance but their preparedness is undermined by a significant lack of proactive measures like risk assessments, staff training, and disaster recovery practices. In agreement with the finding of this study, Alzyadi, et al (2021) found that response practices to mitigate cybersecurity incidents are actions taken to manage threats, reduce damage, and improve future security. In contrast Ershova, et al (2021) found that an effective response involves a comprehensive plan covering preparation, detection, containment, eradication, and recovery.

4 Conclusion

The study concluded that that while university libraries in Katsina State have made initial progress in establishing some foundational cybersecurity protocols, their overall preparedness and response capabilities remain insufficient to address the evolving landscape of digital threats. Recurring issues like unauthorized access, system vulnerabilities, and inadequate staff training further underscore systemic weaknesses in proactive risk management and recovery planning.

Recommendations

The study offered the following recommendations:

1. Library Management should strengthen their cybersecurity monitoring systems to prevent common issues like unauthorized access and network failures. Implementing real-time monitoring systems and regular vulnerability assessments can help identify and mitigate risks related to computer viruses, phishing, plagiarism, and software piracy, which continue to threaten digital information service delivery.
2. Library Management should improve the adoption of cybersecurity preventive measures, particularly strengthening password policies, increasing user education on cybersecurity best practices, and conducting periodic vulnerability assessments. Libraries should also work closely with IT experts to ensure continuous system monitoring and provide regular staff training to raise cybersecurity preparedness and resilience.
3. There is need for library management to refine their response practices by implementing regular risk assessments, establishing proactive early warning systems, and ensuring comprehensive disaster recovery plans. Strengthening encryption practices for sensitive data, improving role-based access controls, and training staff in incident response procedures will enhance the library’s ability to handle cybersecurity incidents swiftly and effectively.

References

Ajie, I. (2019). A Review of Trends and Issues of Cybersecurity in Academic Libraries. *Library Philosophy and Practice (ejournal)*.2523. Retrieved from https://digitalcommons.unl.edu/libphilprac/2523

Akor A, I. Musa, A & Ogunode, N. J (2021).Causes, Forms and Consequences of Insecurity on Nigerian Educational System: Implications for Educational Managers. *Middle European Scientific Bulletin*, (18), 262-272.

Alzyadi, A., Buhari, S. M., &Algarni, A. S. (2021). Cybersecurity Awareness among Library and Information Professionals: A Case Study. *Journal of Librarianship and Information Science, 53(1), 235-248.*
https://doi.org/10.1177/09610006211009692

Chingoriwo T. (2022) Cybersecurity Challenges and Needs in the Context of Digital Development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies*: Engineering and Technology, 3(2), 77-104

Ershova, A., Melekhina, O., &Arkhipova, A. (2021). Cybersecurity as a modern digital library management strategy: Information security in electronic catalogues. *Journal of Interdisciplinary Methodologies and Issues in Science*, 5(2), 30-42.

George, C., & Onyema, J. (2020). Adoption of e-learning and blended learning in university libraries. *International Journal of Library and Information Science*, 12(4), 56-67.

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

Hussain, A., & Ahmad, P. (2021). Adoption of smart technologies in university libraries of Pakistan: a qualitative review. *Library Philosophy and Practice*, 2021, 1-10.

Ibrahim, H. O., & Umar, F. A. (2020). Cybersecurity Threats and Its Emerging Trends on Academic Libraries. *International Journal of Academic Library and Information Science*, 8(2):22-26

Khalipi, A. (2023). Exploring the awareness of security threats associated with short message Service (SMS) and protective measures against SMS security threats amongst students at the University of Namibia (UNAM). *A Thesis Submitted For the Degree of Master of Science in Information Technology of the University of NAMIBIA.*

Lab, K. (2020). *Kaspersky Lab.* Retrieved from Kaspersky Lab:
https://www.kaspersky.ru/resource-center/preemptive-safety/cybersecurity-basics

Luft, P. J., (2020). "Proactive Management in Academic Libraries: Promoting Improved Communication and Inclusion of Academic Librarians and Archivists in Cybersecurity Policy Creation. *Theses and Dissertations.* 421.
https://csuepress.columbusstate.edu/theses_dissertations/421

Mandlenkosi, R. M. & Witness, M (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal Of Research In Business And Social Science* 11(4), 384-396

Masenya, T. M., &Chisita, C. T. (2022). Futurizing Library Services in a Technology-Driven Dispensation: Reflections on Selected Academic Libraries in Zimbabwe and South Africa. In Innovative Technologies for Enhancing Knowledge Access in Academic Libraries (pp. 1-21). IGI Global.

Muhammad, A.A, Daniel, D.W. & Samson I. (2020). An empirical analysis of cybercrime trends and its impact on moral decadence among secondary school level students in Nigeria. *Published in Collaboration with The 26th iSTEAMS*
Bespoke Multidisciplinary Conference, Accra Ghana & The School of IT &
Computing, American University of Nigeria, Yola
www.isteams.net/ghana2020bespoke, 73-84

Musa, S., &Maifata, N. M. (2020). Library security and service delivery in federal university libraries in North Central Nigeria. *Nasarawa Journal of Library and Information Science (NAJLIS)*, 4(1), 45-57.

Museba, T.J., Ranganai, E & Gianfrate, G. (2021). Customer perception of adoption and use of digital financial services and mobile money services in Uganda.

Journal of Enterprising Communities: People and Places in the Global Economy, No. 1.

Ngulube, P. (2019). Digital preservation practices in academic libraries in South Africa in the wake of the digital revolution. *South African Journal of Information Management*, 21 (1), 1–9.

Nikhat, A, Bedine K, Yusuf P, Anurag T, & Sheeba P. (2021). A Comprehensive

Overview of Privacy and Data Security for Cloud Storage. *International Journal of Scientific Research in Science*, *Engineering and Technology* (IJSRSET), 08 (5),113-152. DOI: 10.32628/IJSRSET21852

Okike, B. O. I. & Adetoro, N. (2019). Are There Threats to Information System Security? A Focus on University Libraries in South-West, Nigeria. *Gateway Information Journal* GIJ 20(1) June, 2019 Journal https://www.gatewayinfojournal.org/

Pathak, S. (2019). "Disaster and security preparedness of libraries in India. *Library Philosophy and Practice (e-Journal)*, 1-25

Peter, A. S. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, 17, 4959.

Ryder, R. D. &Madhavan, A. (2019). *Cyber Crisis Management: Overcoming the Challenges in Cyberspace*. Bloomsbury Publishing.

Sust, D., & Vancza, J. P. (2017). Applying the Cybersecurity Capability Maturity

Model (C2M2) in Small Businesses. *Journal of Computer Information Systems*, 57(1), 91-100.

Yusof, M. K., & Saman, M. Y. (2016). The adoption and implementation of RFID: a literature survey. *LIBRES: Library and Information Science Research Electronic Journal*, 26(1), 31.

Yusuf, P., Qamar, S. A., Nikhat, A., Jai, P. D., & Anurag, K. J. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management* (IJSRM) 9(12), 669-710, (e): 2321-3418. www.ijsrm.inDOI: 10.18535/ijsrm/v9i12.ec04

Yusuf, T. I., Adebayo, O. A., Bello, L. A., & Kayode, J. O. (2022). Adoption of artificial intelligence for effective library service delivery in academic libraries in Nigeria. *Library Philosophy and Practice* (e-journal) 6804. https://digitalcommons.unl.edu/libphilprac/6804