International Journal of Information Resource Management (IJIRM)
Volume 3, Number 2 (2026)
E- ISSN: 1118-7786

INFLUENCE OF CYBERSECURITY THREATS ON DIGITAL PRESERVATION OF INFORMATION RESOURCES IN SELECTED LIBRARIES IN CROSS RIVER STATE, NIGERIAN

Isu Michael Egbe
Department of Library and Information Science
Faculty of the Social Sciences, University of Calabar

and

Bernard Beshigim Aniah
College of Health Technology, Calabar, Cross River State, Nigeria

Abstract
The study investigated types of cybersecurity threats and digital preservation of information resources in Nigerian libraries. Three objectives, three research questions and three hypotheses were developed to guide the study. The study used survey research design. The population of the study comprised thirty-five (35) librarians chosen from three libraries in Cross River State. The entire population was used for the study since it was small and manageable. A structured questionnaire was used to gather data for the study. The statistical method employed to test the hypotheses at the .05 level of significance was simple regression analysis. The findings showed that denial-of-service (DoS) attacks, malware attacks, and data breaches had a significant influence on digital preservation of information resources. Based on the findings of the study, it was recommended among others that; the government and non-governmental organizations should provide the needed funds for the procurement of up-to-date ICT facilities in libraries to aid the fight against cyber threats and that the library management should organize awareness programs for library staff to cultivate a security-conscious culture within the library.

Key words: Cybersecurity, Cyber threats, Digital Preservation, Information Resources, Nigerian Libraries

Introduction

The library is the store house of knowledge, it provides equitable access to learning resources, technologies, and environments that bridge gaps between formal, non-formal,

and informal education. For many individuals, especially those with financial, geographic, or social disadvantages, libraries remain the only accessible spaces offering free or low cost learning materials. With the rise of digital learning platforms, open educational resources (OERs), and flexible learning pathways, libraries have expanded their role to include training in digital skills, research skills, information literacy, and soft skills vital for navigating contemporary knowledge ecosystems. Library from time immemorial has been considered as a "social institution". It plays an immense role in the modern society and is regarded as the "gateway of knowledge" for the community. With the generation of new information sources including web-based resources there is a huge change in the role and form of the libraries. Today people in every sphere of the society irrespective of their age, profession, etc. from childhood to adulthood, from teacher to politician, businessmen to housewives use the libraries to satisfy their information needs, hence the need for the resources in the library to be secured (Egbe, Enidiok & Ugbe, 2025; Lison & Reinders, 2020).

Library information resources are essential, curated materials (print and digital) that support research, learning, and teaching, ensuring access to reliable, up-to-date knowledge. Major types include printed books, journals, and newspapers, alongside electronic databases, e-books, and audiovisual materials, all critical for academic and personal development. The major aim of setting up libraries is to encourage and promote readership as well as scholarship. Hence, the library designs its programs of services and provides the necessary information resources to meet the information needs of the clients. It is in light of this that the library endeavors to provide viable information resources.

These information resources transform an individual from a nobody to a somebody. It transforms illiterate community to literate society. For the library to achieve its goal, the people it is meant to serve must be aware of its resources and existence. Information resources in libraries are very important because they are essential for research, teaching, learning, and assignment completion, especially for students and researchers; they function as storehouses of both published and unpublished knowledge, preserving intellectual history; high-quality, reliable, and up-to-date resources (especially e-resources) are crucial for current academic and personal development; and they also provides access to specialized materials that individuals cannot afford or manage on their own, therefore, their preservation is very critical (Egbe, Mbah & Ugbe, 2025).

Digital preservation is the process of preserving rare, delicate objects and items by digitizing them using computers, electronic devices, cellphones, digital cameras, recorders, and digital displays. Preservation techniques are employed to convert old materials into digital format, and digital libraries are collections of records that are made available online in electronic format, using one or more digital preservation approaches. Digital preservation typically aims to maintain, preserve, and make digital content accessible for a long time (Hazarika & Librarian, 2020). In order to keep digital content accessible to customers and future generations for an extended period of time, digital preservation integrates policies, methods, and actions to guarantee the accurate presentation of verified content across time, despite the difficulties posed by media failure and technical progress.

Information resources should be preserved as much as possible so that the information is retained to retain the information therein for a very long time. Many

libraries in developing nations like Nigeria have yet to implement digital preservation of library resources, according to Sambo et al., (2017). Furthermore, as being digital does not always mean that a resource is always available, the shift to a digital world has created significant and urgent challenges, particularly for academic libraries, regarding how to organise, access, and preserve digital materials in perpetuity (Masenya & Ngulube, 2020). Therefore, if digital protection is not given priority and quick action is not taken to save the deteriorating conditions of resources, libraries run the risk of losing important digital information.

Digital preservation of born digital materials as well as materials that were transformed from analog (printed documents) to digital format using cameras, scanners, and other imaging technologies for access and preservation are quickly emerging as a key tool for information creation, storage, and dissemination. Digital preservation is the set of procedures and measures necessary to guarantee consistent and dependable access to authenticated digital information resources for as long as they are thought to be valuable. Another way to think about digital preservation is as a collection of procedures and actions that guarantee ongoing access to data, records, resources, scientific and cultural legacy that are available in digital formats (Gbaje, 2011).

Cybersecurity is like a shield against cyberattacks on internet-connected systems, including data, software, and hardware. Protecting sensitive data, such as research findings, faculty and student records, and digital collections, has become a top priority for libraries. Libraries, particularly those at universities, have a wealth of sensitive information that, if not properly safeguarded, could be abused (Lee, 2022). The integrity, availability,

and confidentiality of vital systems and services are seriously and continuously threatened by cybersecurity flaws in digital infrastructures. Numerous factors, such as software defects, incorrect settings, human mistakes, and the growing interconnectedness of networks and devices, can give birth to these vulnerabilities. To protect digital infrastructures from cyberattacks, it is essential to recognize and fix these vulnerabilities.

The protection of internet-connected systems, including data, software, and hardware, from cyberattacks is known as cybersecurity. Libraries, both academic and public, now place a high premium on protecting sensitive information, including research findings, student and faculty records, and digital collections. Libraries, hold a lot of sensitive data that could be misused if not properly protected (Lee, 2022). Cybersecurity susceptibilities in digital infrastructures provide a major and ongoing danger to the confidentiality, availability, and integrity of critical systems and services. These susceptibilities can be caused by a variety of things, including software flaws, improper configurations, human error, and the increasing interconnection of devices and networks. It is crucial to identify and address these susceptibilities in order to shield digital infrastructures from cyberattacks.

Although the digital era has increased access to information, it has also increased the danger of data breaches and illegal access to private data. Cybersecurity is essential for libraries since they are major centers for research and information exchange. Scholarly communications, institutional reputations, and intellectual property can all suffer greatly from a breach in these systems. "Cybersecurity is not only about protecting library systems from external threats but also about ensuring that the digital rights of users are

maintained," (IFLA, 2022). One of the primary cybersecurity issues in metaverse libraries is the vast amount of data generated by users and the potential misuse of this information. Libraries must implement strong data protection measures, including encryption, anonymization, and compliance with privacy regulations, to prevent breaches and unauthorized access (Oladokun, Ajani, Oloniruha, Ilori, Nsirim, & Egbe, 2025)

Cyberattacks and cyber threats continue to increase in number despite technological innovations and advancement; these include network intrusion, computer virus distribution, identity theft, cyberstalking, cyberbullying, cyberterrorism, and more. Given the realities of these attacks, crimes, and other cyber threats, it is imperative that people, businesses, and organisations that use the internet have security tools or applications in place to guard against these threats, crimes, and attacks, including web jacking, malicious applications, data breaches, and many more (Bhavsar & Bhavsar, 2017). On the other hand, although security tools such as firewalls, encryption, and anti-virus software aid in defending against online threats, attacks, and crimes, they also have a tendency to violate users' privacy by accessing and gathering a lot of data about them, including sensitive data. Therefore, when choosing which protection mechanisms to employ, libraries and their patrons must balance the advantages and disadvantages of security measures and potential privacy invasion.

Protecting data, programs, and computer networks against unauthorized access or attacks is the goal of cyber security measures. The confidentiality and integrity of the data stored on and accessed through these technical gadgets are accommodated by cyberspace security. Reddy and Reddy (2014), enumerated a number of cyber security strategies, such

as firewalls, malware scanners, passwords, access control, and anti-virus software. Additionally, applying program updates as soon as they are made available aids in thwarting or protecting against attacks (Bhavsar & Bhavsar, 2017). This is due to the fact that the majority of updates are designed to fix problems like bugs, vulnerabilities to specific malware, and generally make a software or application better and more secure than the one that came before it. To protect their data, the library and its patrons might also use a strong password that is difficult to figure out.

Statement of the problem

There seems to be increased cyber attacks and threats against libraries which are attributed to user vulnerabilities and a substantial reliance on the internet for daily tasks and activities. Additionally, losses are sustained everyday due to the actions of unauthorised users, referred to as cybercriminals, who exploit internet usage to perpetrate various assaults, including data breaches, malware infections, and denial-of-service (DoS) attacks, thereby impacting digital culture. This has resulted in substantial annual financial losses for libraries and resources. Consequently, safeguarding information resources against assaults has become a primary priority in libraries.

It was observed that significant efforts have been undertaken to guarantee that libraries in Nigeria can access the growing array of digital resources in the future. Numerous initiatives were initiated to promote collaborative endeavours in the preservation of digital assets, while also supplying the necessary infrastructure and enhancing capabilities inside Nigerian university libraries to protect digital resources. Nonetheless, these attempts appear to be ineffectual, as observations indicate that such attacks remain frequent on digital materials in libraries. It is against this backdrop, that the

researchers conducted this study to examine types of cybersecurity threats and the preservation of digital culture in Nigerian libraries.

Research questions

i. What is the influence of data breaches on digital preservation of information resources?
ii. How does malware attacks influence digital preservation of information resources?
iii. To what extent does Denial-of-Service (DoS) attacks influence digital preservation of information resources

Hypotheses of the study

The following hypotheses were used to guide the study.

i. There is no significant influence of data breaches on digital preservation of information resources
ii. Malware attacks does not significantly influence digital preservation of information resources
iii. Denial-of-Service (DoS) attacks does not have any significant influence on digital preservation of information resources.

Literature review

Data breaches and digital preservation of information resources

When sensitive information is accessed by unauthorized parties, data breaches take place. A data breach may expose research materials, copyrighted content, or personal information in the context of digital collections. Hackers may obtain unauthorised access by taking advantage of system flaws. The rising focus of cybercriminals on healthcare companies was thoroughly examined by Ibrahim et al. (2020), since the impact of the attack is not only financial but also jeopardizes the efficiency of patient care delivery. In light of this, the authors stress the fact that threat intelligence about the healthcare sector

is still in its infancy as well as the policy factors that ought to guide data protection efforts. This may have a detrimental effect on the patient information database.

A more thorough examination of data breaches in the healthcare environment, was undertaken by Angst et al. (2017), which supports this rising threat level. According to their research, the frequency of data breaches has been steadily increasing, the cost of each breach has skyrocketed, and a breach involves more than just financial damages. According to this perspective, Marseille (2020), examines the high frequency of data breaches that occur nowadays and also draws attention to the more extensive and long-lasting effects on businesses, including diminished market share, diminished brand image, and diminished organizational reputation. The second main indicator of the present security threat levels is the continuous growth of contemporary data breach techniques, which is one of the major trends. Cheng et al. (2017), investigated enterprise data breach causes, associated challenges, and best practices to prevent them, their findings, indicated that the evolution of cybercriminals has led to the emergence of increasingly complex threats. Kostic (2020), examined the position of information security awareness tactics as a weapon against social engineering techniques, which the author considers to be one of the most popular and effective attack vectors. In order to prevent these attacks, libraries must implement sufficient security measures for their resources. A thoughtful explanation of how to protect consumer data collection by defining security standards, enforcing privacy laws, introducing personal identity setup, and adjusting public identification numbers was provided by Marcus (2018). Cheng et al. (2017), suggested several data breach prevention

measures, including data encapsulation, data coding, and network intrusion detection system implementation.

An investigation on the relationship between data vulnerability and technological advancement, was carried out by Wang et al. (2023), focusing on the need for effective risk mitigation and the adoption of new, cutting-edge security techniques and technologies. Bhadouria (2022), emphasised the significance of protective methods that would incorporate organizational, social, and technical enablers while analyzing the effects of malicious assaults and data breaches. Informational services and IT solutions play a major role in the operations of current organizational structures. The vulnerability of many firms' IT profiles has expanded dramatically due to the growing use of cloud solutions, teleworking, and BYOD regulations. As a result, while these developments encourage better workforce capabilities to generate value and advance ideas, IT has also witnessed significant explosions in data security vulnerabilities due to increased exposure. Threat actors used to be kept within an organisation's physical boundaries and defenses, but these days, threat vectors have spread into networks, necessitating security measures in libraries to preserve their cultural legacy.

Malware attacks and digital preservation of information resources

Malware is a general word that includes all forms of malicious software, such as computer viruses, worms, Trojan horses, spyware, logic bombs, keyloggers, shareware, backdoors, botnet code, and root kits, (Conrad et al., 2015). Digital collections can become infected with malware, including ransomware, worms, and viruses. Malicious software can interfere with operations, corrupt or destroy data, or jeopardize the availability and

integrity of the collection. Particularly, ransomware attacks have the ability to encrypt data and demand a fee to unlock it, resulting in serious interruptions (Egbe, Ugbe & Enu, 2025). University and public libraries are especially susceptible to malware assaults because they frequently grant the general public access to computers and digital resources. Through downloads, e-mails, or compromised websites, malware, which can be viruses, worms, or Trojan horses, can attack library systems (Onifade, 2022). Malware can destroy data or steal private information after it is installed, which makes it hard for libraries to function properly. Systems and networks in libraries may become infected with malicious software, or malware, which could harm them or grant unwanted access to private data. Spyware, ransomware, and viruses are common forms of malware. Libraries are susceptible to malware attacks that compromise user data, interfere with library services, or steal intellectual property.

Like technology itself, cybersecurity is essential to our way of life. In actuality, they are inseparable, and technology has come to define our culture. According to Ajie (2019), security is the most important issue facing higher education institutions because of the growing amount of information available. Cyber threats have also affected academic libraries in the information age, which has led to the development of cybersecurity. Library security policies, procedures, and plans are used to protect library resources from attacks. Cybersecurity also reiterates concerns about protecting cyberspace from attacks like cyber threats and malicious use of information. The main goals of cybersecurity are defense against intrusion and protection of network systems against unauthorised access and data alteration from within.

During the 2000s, there were approximately 37,000 attempted attacks on government and private enterprises, as assailants enhanced their strategies by employing zombie computers—compromised machines connected to the internet that relay transmissions to obfuscate the origin of the attacks (Radware, 2017). To take control of a system, attackers can employ a variety of malware, viruses, and worms (Harris & Maymi, 2016). The infection affects both the system as a whole and the integrity of data or information that has been stored. Destructive software is used by malware attackers to carry out actions that could compromise electronic communication. Malware tools can alter how a victim receives content. Malware is becoming more sophisticated, and it may frequently enter its target system undetected in order to collect data. Malware programs collect personal information, store and disseminate illicit content, and target computer and network systems, (Pinguelo & Muller, 2011). Malware programs have the ability to attack and destroy infrastructures in addition to personal PCs. These malwares have the potential to seriously harm digital content in unprotected libraries.

Denial-of-Service (DoS) attacks and digital preservation of information resources

The goal of denial-of-service (DoS) assaults is to overwhelm a system's resources so that authorized users cannot use it. These kinds of attacks have the potential to interfere with access to digital collections, depriving the public, students, and researchers of important resources. Attacks such as Distributed Denial-of-Service (DDoS) are very powerful because they involve flooding the target with several systems. DoS attacks can have a significant effect on university libraries, which offer online access to a variety of resources, such as databases, electronic journals, and catalogs. Research and academic

work may be delayed by such attacks, which can momentarily stop access to vital academic resources (Okoye & Olatunji, 2023). According to Kaur, Kumar, and Bhandari (2017), the DoS assault rate increased to 300 Gb per second in 2013. DoS attacks rose to 57% in the fourth quarter of 2014 over the same period in 2013. Many internet connections were brought down by the 2016 DoS attack. 1.2 Tbps was the attack's magnitude.

Researchers tried to more accurately categorize DoS security attacks on businesses, such as electronic warfare, cyber-infrastructure, infiltration, and bandwidth flooding attacks (Harris & Maymi, 2016). Somal and Virk (2014) analyzed the patterns, tactics, and history of a variety of denial-of-service assaults and grouped them according to attack impact, assault speed, and mechanization level. The paper outlined the several strategies put forth to combat DoS assaults and showed how they have grown to be a complicated and significant issue for libraries.

DoS attack operations can take many different forms and frequently take place over a long period of time. Their complexity and diversity have created security issues for libraries. Attackers target and take over computers using a variety of techniques. DoS attacks that send excessive traffic to a network address are ineffectively defended against by conventional security tools like firewalls, intrusion detection systems, and antivirus software. DoS attack operations can take many different forms and frequently take place over a long period of time. Their complexity and diversity have created security issues for businesses. Attackers target and take over computers using a variety of techniques. DoS attacks that send excessive traffic to a network address are ineffectively defended against

by conventional security tools like firewalls, intrusion detection systems, and antivirus software (Harris & Maymi, 2016).

The complexity of DoS attacks on businesses' systems has increased over time, according to Anstee (2013). These attacks happen multiple times a day and at speeds higher than 10 and 20 gigabytes per second (Gbps). Anstee's description and Schwartz's (2013), account of the rise in DoS attacks were similar: 10% of all DoS attempts surpass 60 Gbps, and the average attack speed has risen from 6 Gbps to 48 Gbps. Businesses may suffer financial losses as a result of the rise in frequency and intensity of DoS assaults. Instead of compromising the confidentiality and integrity of the data, DoS attackers often concentrate on sending a deluge of packets (Kashyap & Jena, 2012). This means that libraries need to protect their resources against these attacks for posterity.

Researchers looked at the nature of DoS in different ways, despite the fact that they all agreed that DoS assaults require server disruption. Although Patel and Borisagar (2012), created the DoS taxonomy, Mahjabin et al. (2017), explored the many types, tactics, and procedures of DoS as well as the architectures employed in attacks. Harris and Maymi (2016), examined the DoS attack's operational mechanisms. In a broader sense, Yu (2014), gave insight into the new problems in the field of DoS assaults and details about how DoS attackers carry out their objectives. For the benefit of future generations, libraries are being urged to safeguard their digital materials.

Methodology

The study employed a survey research design. The research was conducted in three libraries in Cross River State: the University of Calabar Library, the National Library of

Nigeria (Calabar branch), and the Cross River State Public Library in Calabar. Purposive sampling technique was used for the study. The study population comprised thirty-five (35) librarians. The population was small and manageable; hence, the entire population served as the study sample. Of the thirty-five (35) questionnaires distributed, only 32 were deemed valid and utilised for the study, resulting in a return rate of ninety-one percent (91%). Simple regression analysis was the statistical method employed to test the hypotheses at .05 level of significance.

Results and Discussion

Hypothesis One

Data breaches has no significant influence on the preservation of digital culture. The independent variable in this hypothesis is data breaches, whereas the dependent variable is the preservation of digital culture. Simple regression analysis was utilised to test this hypothesis. The analysis results are presented in Table 1.

Table 1
Simple regression result of the influence of data breaches on preservation of digital culture (N=32)

Model	**R**	**R. square**	**Adjusted R. square**	**Std error of the estimate**	
1	.917(a)	.841	.835	1.28111	
Model	Sum of square	df	Mean square	F	**p-value**
Regression	259.731	1	259.731	158.253	**.000(a)**
Residual	49.237	30	1.641		
Total	308.969	31			
Variables	Unstandardised regression weight B	Standardised regression weight	Beta weight	T	**p-value**
(Constant)	-3.781	3.173		-1.192	**.000**
Data breaches	**1.849**	**.147**	**.917**	**12.580**	**.000**

*Significant at .05 level.

The simple regression analysis of the influence of data breaches on the preservation of digital culture "yielded a coefficient of multiple regression (R) of .917 and a multiple regression R-square (R^2) of .841 and an adjusted R^2 of .835. The adjusted R^2 of .835 indicated that the Data breaches account for 83.5% of the variance in preservation of digital culture in the study area. This finding is a critical indication that data breaches are relatively high in the area of the study. The F-value of the Analysis of Variance (ANOVA) obtained from the regression table was F = 158.253 and the sig. value of .000 (or p<.05) at the degree of freedom (df) 1 and 30". The implication of this result is that data breaches is a significant predictor of preservation of digital culture. The identified equation to understand this relationship was that preservation of digital culture = -3.781 +1.849 (data breaches). The finding of this hypothesis is in line with the view of Angst et al. (2017), who undertook a more thorough examination of data breaches in the healthcare environment, which supports this rising threat level. According to their research, the frequency of data breaches has been steadily increasing, the cost of each breach has skyrocketed, and a breach involves more than just financial damages.

Hypothesis Two

Malware attacks does not significantly influence preservation of digital culture. The independent variable in this hypothesis is malware attacks; while the dependent variable is preservation of digital culture. Simple regression analysis was employed to test this hypothesis. The result of the analysis is presented in Table 2.

Table 2
Simple regression result of the influence of malware attacks on preservation of digital culture (N=32)

Model	R	R. sqaure	Adjusted R. squared	Std error of the

				estimate	
1	.926(a)	.857	.853	1.21244	
Model	Sum of square	df	Mean square	F	**p-value**
Regression	264.868	1	264.868	180.181	**.000(a)**
Residual	44.100	30	1.470		
Total	308.969	31			
Variables	Unstandardised regression weight B	Standardised regression weight	Beta weight	t	**p-value**
(Constant)	-1.187	2.781		-.427	**-673**
Malware attacks	**1.736**	**.129**	**.926**	**13.423**	**.000**

* Significant at .05 level.

The simple regression analysis of the influence of malware attacks on the preservation of digital culture "yielded a coefficient of multiple regression (R) of .926 and a multiple regression R-square (R^2) of .857 and an adjusted R^2 of .853. The adjusted R^2 of .853 indicated that the malware attacks accounted for 85.3% of the variance in preservation of digital culture in the study area. This finding is a critical indication that malware attacks is relatively high in the area of the study. The F-value of the Analysis of Variance (ANOVA) obtained from the regression table was F = 180.181 and the sig. value of .000 (or $p<.05$) at the degree of freedom (df) 1 and 30". The implication of this result is that malware attacks is a significant predictor of preservation of digital culture. The identified equation to understand this relationship was that preservation of digital culture = -1.187 + 1.736 (malware attacks). The finding of this hypothesis is in line with the view of Conrad et al. (2015), who observed that, malware is a general word that includes all forms of malicious software, such as computer viruses, worms, Trojan horses, spyware, logic bombs, keyloggers, shareware, backdoors, botnet code, and root kits, according to the authors, digital collections can become infected with malware, including ransomware, worms, and

viruses. Also, Onifade (2022), stated that, malware can destroy data or steal private information after it is installed, which makes it hard for libraries to function properly.

Hypothesis Three

Denial-of-Service (DoS) attacks does not significantly influence preservation of digital culture. The independent variable in this hypothesis is denial-of-Service (DoS) attacks; while the dependent variable is preservation of digital culture. Simple regression analysis was employed to test this hypothesis. The result of the analysis is presented in Table 3.

Table 3
Simple regression result of the influence of denial-of-Service (DoS) attacks on preservation of digital culture (N=32)

Model	**R**	**R. square**	**Adjusted R. square**	**Std error of the estimate**	
1	.785(a)	.617	.604	1.98727	
Model	Sum of square	df	Mean square	F	**p-value**
Regression	190.491	1	190.491	48.235	**.000(a)**
Residual	118.478	30	3.949		
Total	308.969	31			
Variables	Unstandardised regression weight B	Standardised regression weight	Beta weight	t	**p-value**
(Constant)	13.129	3.316		3.959	**.000**
Denial of service (DoS) attacks	**1.078**	**.155**	**.785**	**6.945**	**.000**

* Significant at .05 level.

The simple regression analysis of the influence of denial-of-service (DoS) attacks on the preservation of digital culture "yielded a coefficient of multiple regression (R) of .785 and a multiple regression R-square (R^2) of .617 and an adjusted R^2 of .604. The adjusted R^2

of .604 indicated that the denial-of-Service (DoS) attacks accounted for 60.4 % of the variance in preservation of digital culture in the study area. This finding is a critical indication that denial-of-Service (DoS) attacks is relatively high in the area of the study. The F-value of the Analysis of Variance (ANOVA) obtained from the regression table was F = 48.235 and the sig. value of .000 (or p<.05) at the degree of freedom (df) 1 and 30". The implication of this result is that denial-of-Service (DoS) attacks is a significant predictor of preservation of digital culture. The identified equation to understand this relationship was that preservation of digital culture = 13.129 + 1,078 (Denial-of-Service (DoS) attacks). The finding of this hypothesis is in line with the view of Harrison (2000), who posited that the majority of American companies are still being targeted by DoS attacks. The targeted attack rates for CNN, Yahoo, and Amazon were approximately 1 gigabit per second. Clarke and Knake (2010), also stated that DoS attacks are asymmetric, covert, and dynamic; a person, organization, or state from anywhere in the world can block access to or compromise a computer system. Attacks can happen fast and at any time in a global system.

Recommendations

On the basis of the findings of this study, it was recommended that:

1. The government and non-governmental organisations should provide the needed funds for the procurement of up-to-date ICT facilities in libraries to aid the fight against cyber threats.
2. The library management should organise awareness programs for library staff to cultivate a security-conscious culture within the library.

3. There should be regular updates and configurations of security devices to keep pace with emerging threats, ensuring that systems remain effective against new attack vectors.

4. They should be training and re-training of library staff in the area of Information and Communication Technologies (ICTs), to meet up with new trends in information delivery.

Conclusion

The findings of this study indicated that data breaches, malware attacks and denial-of-service (DoS) attacks significantly influence the preservation of information resources. The activities of cybercriminals in libraries is on the rise, libraries are responsible for the preservation of information resources for future generations of users. Therefore, there is need for awareness of these threats by librarians in order to equip them with the requisite knowledge needed to combat these threats.

References

Ajie, I. (2019). A review of trends and issues of cybersecurity in academic libraries. *Library Philosophy and Practice*, *online journal*.

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS quarterly, 41*(3), 893-A8. https://www.jstor.org/stable/26635018

Anstee, R. P. (2013). A survey of forbidden configuration results, *Elec. J. of Combinatorics*, 20, DS20, 56.

Bhadouria, A. S. (2022). Study of impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. *International Journal of Scientific and Research Publications, X*, (X), ISSN 2250-3153. DOI: 10.29322/IJSRP.X.2022.p091095 http://dx.doi.org/10.29322/IJSRP.X.2022.p091095

Bhavsar, S., & Bhavsar, S. (2017). Cybercrimes and measures to prevent in libraries. *Knowledge Librarian, 3*(5), 38-47. Retrieved August 2, 2025, from http://www.klibjlis.com/4.5.7.pdf

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7*(5), e1211. https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/widm.1211

Conrad, E., Misenar, S., & Feldman, J. (2015). *CSSI study guide* (3rd ed.). Waltham, MA: Syngress.

Egbe, I. M., Enidiok, M. S. & Ugbe, M. E. (2025). Challenges and prospects of implementing artificial intelligence in the library environment in Nigeria: Perception of personnel of academic libraries in Cross River State. *Journal of Information, Communication and Media Research*, 1(2), 25 - 35, https://credence-publishing.com DOI: http://doi.org/10.47524/jicmr.v1i2.36

Egbe, I. M., Ugbe, M. E. & Enu, C. B. (2025). Digital violence against women in Nigeria: Strategies for prevention. *The Catalyst Journal of Library and Information Literacy* 4(2), https://journals.journalsplace.org/index.php/CJLIL

Egbe, I. M., Mbah, R. & Ugbe, M. E. (2025). Online databases and utilization of information resources by post-graduates students in the University of Cross River State, Calabar, Nigeria. *Journal of Library Technology and Information Management (J-TIM)*, 1(1); 22-31.

Gbaje, E. S. (2011). Digital preservation policy and implementation strategies for national information centres in Nigeria. Ph.D thesis, Faculty of Education: Ahmadu Bello University Zaria. http://hdl.handle.net/123456789/4130

Harris, S., & Maymi, F. (2016). *CISSP all-in-one exam guide* (7th ed.). New York, NY: McGraw Hill & Osborne.

Hazarika, R., & Librarian, A. (2020). Digital Preservation in Academics Libraries. *International Journal of Library and Information Studies, 10*, (2). http://www.ijlis.org

Ibrahim, A., Thiruvady, D., Schneider, J. G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. *Front Comput. Sci. 2*:36. DOI: 10.3389/fcomp.2020.00036

IFLA (2022). IFLA Statement on Privacy in the Digital World. International Federation of Library Associations and Institutions.

Kashyap, B., & Jena, S. K. (2012). DDoS attacks detection and attacker identification. *International Journal of Computer Applications, 42*(1), 28-33. doi:org/10.5120/5657-7549

Kaur, P., Kumar, M., & Bhandari, B. (2017). A review of detection approaches for distributed denial of service attacks. *System Science and Control Engineering, 5*(1), 301-320. doi.org/10.1080/21642583.2017.1331768

Kostic, L. C. (2020). Information security awareness techniques that reduce data breaches caused by social engineering attacks (Doctoral dissertation, Capella University).

Lee, S. (2022). The impact of cybersecurity threats on academic libraries. *Journal of Library Technology, 39*(4), 120-134.

Lison, B., & Reinders, K. (2020). Libraries and employability: The European perspective. Public Library Quarterly, 39(3), 229–247.

Marcus, D. J. (2018). The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. *Duke LJ, 68*, 555.

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks, 13*(12). DOI:10.1177/155014771774146

Masenya, T. M. & Ngulube, P. (2020). Factors that influence digital preservation sustainability in academic libraries in South Africa. *South African Journal of Libraries and Information Science, 86*(1), 52–63. https://dx.doi.org/10.7553/86-1-1860

Marseille, E. (2020). The rapid growth of data breaches in today's society (Master's thesis, Utica College). https://search.proquest.com/openview/3a55a67d9c495528627ddb5dd389fdd7/1?pq origsite=gscholarandcbl=51922anddiss=y

Okoye, I. E., & Olatunji, S. A. (2023). Data protection and privacy in Nigerian higher institutions: Compliance with the NDPR. *Journal of Data Protection, 9*(1), 78-95.

Oladokun, B. D., Ajani, Y. A., Oloniruha, E. A., Ilori, O. O., Nsirim, O. & Egbe, I. M. (2025). Cybersecurity issues in the metaverse libraries. *Business Information Review, 0* (0) 1–8. sagepub.com/journals-journals.sagepub.com/home/bir DOI: 10.1177/02663821251328826

Onifade, T. (2022). Digital transformation and cybersecurity risks in African academic libraries. *African Journal of Information and Communication Technology, 18*(3), 35-47.

Patel, C. M., & Borisagar, V. (2012). Survey on taxonomy of DDoS attacks with impact and mitigation techniques. *International Journal of Engineering Research & Technology), 1*(9). www.ijert.org

Pinguelo, F. M., & Muller, B. W. (2011). Virtual crime, real damages: A primer on cybercrimes in the United States and efforts combat cyber criminals. *Virginia Journal of Law & Technology, 16*(1). Retrieved from http://ellblog.com/wpcontent/uploads /2012/04/Pinguelo UVA%20JoLT%20Spring%202011.pdf

Radware (2017). History of DDoS attacks. Retrieved on July 15, 2025, from ttps://security.radware. com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/

Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends latest technologies. *International Journal of Engineering and Technology 4*, (1) ISSN: 2049-3444. https://www.researchgate.net/publication/260126665

Sambo, A. S., Urhefe, E. A., & Ejitagha, S. (2017). A survey of digital preservation challenges in Nigerian libraries: Librarians' perspectives. *International Journal of Digital Curation 12*(1),117-128. http://dx.doi.org/10.2218/ijdc.v12i1.426

Somal, K. L., & Virk, S. K. (2014). Classification of distributed denial of service attacks – architecture, taxonomy and tools. *International Journal of Advanced Research in Computer Science & Technology, 2*(2). Retrieved from http://www.ijarcst.com/doc/vol2-issue2/l_k_somal.pdf

Schwartz, M. J. (2013). DDoS attack bandwidth jumps 718%. Information Week. Retrieved on 5th August, 2025 from http://www.informationweek.com/attacks/ddos attackbandwidthjumps-718-/d/d-id/1109576

Wang, Q., Ngai, E. W., Pienta, D., & Thatcher, J. B. (2023). Information technology innovativeness and data breach risk: A longitudinal study. *Journal of Management Information Systems, 40*(4), 1139-1170. https://www.tandfonline.com/doi/abs/10.1080/07421222.2023.2267319

Yu, S. (2014). *Distributed denial of service attack and defense*. New York, NY: Springer.