

Awareness and perception of cybersecurity among librarians in federal universities in South-West, Nigeria

¹Omoike Adenike and ²Alabi Raliat

¹Kenneth Dike Library, University of Ibadan

² Faculty of Law Library, Fountain University, Osogbo

Abstract

This study investigated awareness and perception of cybersecurity among librarians in federal universities in South-West, Nigeria with the aid of descriptive survey research approach. Questionnaire was used to elicit information from 179 librarians and system librarians, out of which 167 (93.3%) copies of the questionnaire were duly completed and returned. The data collected were analyzed using frequency count, percentages and Pearson Product Moment Correlation analysis to test for the significant relationship between awareness and perception of cybersecurity among librarians tested at 0.05 level of significance with the aid of SPSS Version 21. The study revealed that the level of awareness of cybersecurity among librarians in Federal Universities in South-West, Nigeria is moderate. The findings also revealed that to a high extent are librarians in federal universities in South-West, Nigeria are aware of the potential cyber threats and attacks to library resources. The study showed that librarians perceived that deliberate attack to destroy sensitive data in the library database is unjust (mean=1.62), the use of the computer in committing crimes is unjust (mean=1.61) and that having an unauthorized access to data and other computerized systems (hacking) is considered unjust (mean=1.56). The study revealed that hardware skill (mean= 3.21), software skill (mean=3.10), operating system skills and programming language skills (mean=3.01) were the main librarians' information technology skills to secure library resources. The study further showed that librarians make use of technical security measures in the libraries through access control and password security (mean=3.26), through video surveillance (CCTV system) (mean=3.25) and through installation of updated software (mean=3.11); and the use of non-technical security measures in libraries are through burglary protection and fire extinguishers (mean=3.16) and architectural considerations (mean=3.07). The study also showed that crashing of a computer due to virus, malware, hackers etc (mean=2.99), lack of fund (mean=2.94) and lack of trained information technology (IT) manpower (mean=2.91) were the main challenges encountered in securing information resources against cyberattacks by librarians. There is no significant relationship between awareness and perception of cybersecurity among librarians in Federal Universities in South-West Nigeria. The study recommended that Government should provide adequate fund for universities to run their library effectively. Many universities experiences lack of fund to improve their library. Meanwhile, to provide appropriate security measures in libraries, there is a need of availability of funds.

Keywords: Awareness, perception, cybersecurity, librarians, federal universities, South-West, Nigeria

Introduction

The impact of Internet on library services are in technical processing, collection development, interlibrary loan, reference service, information service, information retrieval, user education, marketing of library services and security of library resources and services. Security of library resources is a sine qua non, Internet users and institutions are vulnerable to cybercrime, threats and attacks and the only solution is cybersecurity for protection of

resources from unauthorised users and attackers. To sustain cybersecurity practices in library, librarians must have full awareness of forms of cybercrimes affecting library information resources.

Awareness could be the pre-informed knowledge of librarians about the unscrupulous activities of cyberhackers that can distorts the information services provision in the library. Therefore, librarians needs to exercise their professionalism in the library. They must be technology inclined to

fight against cybercrime that can affect the growth of the library. However, as much as the Internet provides easy life for humanity, some unscrupulous elements are interfering with activities of the people using the Internet, some with genuine intention, some have bad intent, this necessitate the security and protection of data and information on the Internet, the process of protecting and safeguarding information on the internet is known as cybersecurity.

Nevertheless, the way librarians perceived the issue of cybersecurity determines to what extent librarians address the issue of cybersecurity in the library. Kerkhofs (2018) defined cybersecurity as technologies and processes designed to protect computers, networks and data from unauthorised access, vulnerabilities and attacks delivered via the internet by cybercriminals. The activities of these unscrupulous elements are known as cybercrime, the computer systems is vulnerable to different attacks, some of these attacks are malware, phishing, social engineering and denial of service as mentioned by different literature and authors.

Library and librarians as custodians of information resources should be aware of the various threats to resources in their custody and provide adequate security to prevent unauthorised use and damage to library materials. Information security is a sub set of cybersecurity which deals with only security of information, on the other hand, cybersecurity is more encompassing, looking at the security of both data, processed information and networks including computer systems.

Statement of the problem

Extant literature has revealed that there is increase in cyber-attacks and threats across the world due to vulnerabilities of users of Internet and predominant reliance on

internet to carry out daily functions and activities. Also, in academic libraries, losses are incurred on daily bases as a result of activities of unauthorised users known as cybercriminals through the Internet usage causing all forms of attacks, phishing, malware, identity theft are examples of attacks to cyberspace. This has caused loss of huge amount of money to be expended yearly on digital libraries and resources. As a result, protection of information resources from attacks has been a major concern in the library. Study by Ajie (2019) on a review of trends and issues of cybersecurity in academic libraries, affirmed that librarians' awareness, knowledge and perception about cybersecurity are very low. This serves as a gap that this study intends to fill to gear up librarians to wake up to their responsibilities in the area of cybersecurity in Nigeria. The study therefore investigates awareness and perception of cybersecurity among librarians in Federal university libraries in South-West, Nigeria.

Objectives of the study

The broad objective of the study is to investigate awareness and perception of cybersecurity among librarians in Federal Universities in South-West, Nigeria. The specific objectives are to:

1. examine the level of awareness of cybersecurity among librarians in Universities in South-West, Nigeria;
2. examine whether librarians are aware of the potential cyber threats and attacks to library resources;
3. determine how librarians perceive the issue of cybercrime in university libraries in South-West Nigeria;
4. determine whether librarians have information Technology skills to secure library resources;
5. explore whether librarians in universities make use of both

technical and non-technical security measures in libraries;

6. investigate the challenges encountered in securing information resources against cyberattacks.

Research questions

The following research questions were raised to guide the study:

1. What is the level of awareness of cybersecurity among librarians in universities in South-West, Nigeria?
2. To what extent are librarians in universities in South-West, Nigeria aware of the potential cyber threats and attacks to library resources?
3. What is librarians' perception on the issue of cybercrime in university libraries in South-West Nigeria?
4. What are librarians' information technology skills to secure library resources?
5. How do librarians in universities make use of both technical and non-technical security measures in libraries?
6. What are the challenges encountered in securing information resources against cyberattacks.

Hypothesis

The following null hypothesis is tested at 0.05 level of significance in the study:

Ho1: There is no significant relationship between awareness and perception of cybersecurity among librarians in federal universities in South-West, Nigeria

Literature review

The field of cybersecurity is becoming important due to reliance on computer systems, internet, wireless network, Wi-Fi, smartphones, televisions and other devices constituting internet of things. Cybersecurity is the protection of cyberspace from attack, damage, misuse and economic espionage of

our critical infrastructure are agriculture, commercial facilities, dams, energy, information technology, shipping, banking, defence and education. Rouse (2019) defined cybersecurity to be protection of internet connected systems including hardware, software and data from cyberattacks. In a computing context, protection or security means security against unauthorized access to data and other computerized systems, information security is designed to maintain confidentiality, integrity and availability of data. Common types of cybersecurity are network security to protect network traffic by controlling incoming and outgoing connections to prevent threats from entering or spreading on the network, data loss prevention and cloud security.

Symantec (2019) stated that cybersecurity is the process of protecting and recovering networks, devices and programs from cyber-attack because cyberattacks are evolving danger to organisations, employees and consumers, designed an attack to access or destroy sensitive data or extort money, destroy businesses and damage people's financial and personal lives. Wong (2016) noted that cybersecurity is vital to our way of life as technology itself. In fact, they cannot be separated and indeed the fabric of our society is now defined by technology. Adesina (2017) opined that the advent of computers and the internet has opened a vast array of possibilities for the young and the old in the international community to have access to the world from their homes, schools and offices. Libraries all over the world keep data and information about their users and patrons, details of users such as full names, place of work, credit cards details, phone numbers are data collected by libraries before patrons can access resources of the libraries, however, hackers can sniff into the library data to collect information

about users, more often than not, users may be denied access to the library resources and resources borrowed from the library may stay longer than normal with users of library due to access denial or disruption of such library data.

Ajie (2019) postulated that security top the list of issues affecting higher education institutions considering the increasing volume of information available and that in information age, cyber threats have plagued academic libraries thereby causing the emergence of cybersecurity and that library security policies, procedures and plans are used to protect library resources from attack, further reiterates that cybersecurity is concerned making cyberspace safe from attack such as cyber threats, malicious use of information and that major objective of cybersecurity are protection of network system against unauthorized access and data alteration from within and defense against intrusion.

According to Ajie (2019) citing Davies (n.d), cybersecurity is related to information security, highlighted cybersecurity measures as safety actions that academic libraries can adopt to be installation of updated software, run anti-virus software, malware scanners, turn on firewalls protective barriers between computers and the internet, avoid spyware, protect passwords and back up important files to reduce risk of losing important information to virus, thefts and hackers. Ifeoma (2019) explained that cybersecurity is a technology designed to protect networks, computers programs and data from attack, damage or unauthorized access and that in the past theft and defacement were common threats to physical resources in the library, libraries are digital in nature exposed to cyber threats have plagued academic libraries making it necessary for the emergence of cybersecurity.

According to Usman and Gopakumar (2018), all library professionals have to acquire IT skills, mainly in three areas of information technology, i.e. hardware, software and web applications. As electronic resources too have become part of library resources, the management of electronic resources becomes the responsibility of librarian. Knowledge in three areas of information technology is indispensable for a library professional because he/she has to make use of all the possibilities of information technology in order to provide the users the best service including print and electronic resources, as the time demands.

Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims (Adesina, 2017; citting Clough, 2010). They further noted that the proliferation of digital technology, and the convergence of computing and communication devices, has transformed the way in which we socialize and do business. While overwhelmingly positive, there has also been a dark side to these developments. Proving the maxim that crime follows opportunity, virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes. Thus, one major consequence of this unlimited access to the world has been an increase in the spate of cybercrimes.

Singh and Margam (2018) considered Radio Frequency Identification (RFID) to be the latest technology being used in libraries for self-checkout and check in, book identification, sorting and conveying of library books and for theft detection. They further opined that the technological security refers to the security of library software, hardware, network security, server security, data security, workstations security and electronic security systems such as RFID, Fire alarms, Burglary protection and barcode, etc. Tangential

issues such as data Sovereignty, digital trails, and leveraging technology talent. Cybersecurity is not optional. It must form part of the design of every product, of every database, of every electronic communication. And through education, awareness, and proactive change we can all play a part in securing our future. Newby (2014) stated that libraries are connected to the internet without personnel specifically responsible for managing the security of the library from intrusion, breach and threat, recommended that someone should be responsible for the management of security of e- resources in library.

According to Adesina (2017), technology and the data it depends on can be turned against us, when you read yet another report of a multimillion-dollar bank theft, yet another million usernames and passwords leaked on the web, or yet another scam milking millions from vulnerable people, what you are reading about is the lack of cybersecurity a failure to protect systems, processes, or data and thereby enabling exploitation. Sometimes the end result is just an embarrassment for a company or individual; at other times it can cause significant financial or operational harm. At its worst, loss of life can be a result.

According to Blackwood-Brown (2018), cybersecurity awareness refers to educating internet users about cybersecurity issues, benefits, threats and attacks that can jeopardize their activities on the web, mitigate action against attack and how to prevent unauthorised users. Ray (2019) explains that users of internet should take the following precautions, installing anti-virus software, firewall, securing wireless networks and using spam filters. Mark and Ray (2019) stated that attacks continue to increase on social engineering relying on weaknesses of individuals as a means of gathering information and cybersecurity are

reshaping the lives of users, cybersecurity has changed how users interact with technology. (Ray, 2019; Elson, 2017) attackers use tricks to access personal information from users, passwords of users need not be known, a little information about user is enough to withdraw money from their accounts, automated teller machine (ATM) can dispense cash without valid card.

Zhang and Bryant (2009) explained that security perception and security practice to include usage of antivirus software, firewalls, passwords, email security habits and security education are important to users of internet. In the world of Yahn (2018) cyberattacks can be categorized into spam, phishing, denial of service, IP spoofing, social engineering spyware, malware and viruses, such as Trojan, worm, Bot, Botnet, Key logger all these come within the realm of cybercrime. Educating employees through cybersecurity awareness programme ultimately contributes to organisation's cybersecurity efforts and that employees risky online behaviour are responsible for many attacks, new business opportunities online, cloud and social media are privileged vectors to reach a wide audience unaware of cyber threats (Kolb and Abdullah 2009, Paganini 2013, Ray 2014).

Newby (2014) averred that libraries have made significant investment in computer based resources, training and services, however such investments need to be protected from abuse, misuse by taking active role in cybersecurity. Fischers (2016) gave the following as challenges of cybersecurity to be attack which compromise the confidentiality, integrity and availability of ICTs system, cyber theft or cyber espionage can result in exfiltration of financial, proprietary or personal information from which the attacker can benefit without knowledge of victim, denial

of service can prevent legitimate users from accessing a system.

Methods

The research design adopted for this study was descriptive survey research approach. This was selected as the most appropriate design to obtain accurate assessment of the characteristics of whole populations of people (Kerlinger, 2000). The respondents were librarians and system librarians working in university libraries in Federal universities in South-West Nigeria. The study population was the whole federal universities in South-West Nigeria. A total of 179 questionnaires were distributed, out of which 167 were returned. There were, however, some missing data points due to few unanswered questions by respondents. The research instrument was a standardised scale adopted from well-known scholars and the reliability coefficient for awareness of cybersecurity among librarians was found to be $\alpha=0.76$, perception of cybersecurity among librarians was found to be $\alpha=0.72$ and the reliability coefficient between variables was found to be $\alpha=0.84$ using Cronbach's alpha method.

Results

Data were analysed as they related to the specific areas of the study using descriptive

and inferential statistics such as frequency distributions, percentages and correlation analysis to test for the significant relationship between variables.

A total of 179 copies of the questionnaire were administered to respondents in the university libraries out of which 167 copies were duly completed and returned and were founded valid for analysis. This represents a total of 93.3% response rate as revealed in Table 1, which is a very good result.

Table 2 shows that out of the 167 respondents, majority 86(51.5%) were between 36 and 45 years of age, followed by 62(37.1%) respondents who were within 26-35 years of age, while 11(6.6%) of the respondents were between the age of 56 and above. About 6(3.6%) were within ages 46-55 years. While, just only 2 (1.2%) were within ages 18-25 years. The result indicated that majority of the librarians are matured in age.

Table 3 reveals that a majority 88 (52.7%) of the respondents were female while the remaining 79 (47.3%) were male. These respondents cut across all the federal university libraries.

Table 4 shows that majority of the respondents 122 (73.1%) were married, while the remaining 45(26.9%) of them were single.

Table 1: Questionnaire response rate

S/N	Name of universities	Sample	Return	Percentage (%)
1	University of Lagos, Akoka	23	21	12.6
2	Obafemi Awolowo University, Ile-Ife	22	20	11.9
3	University of Ibadan, Ibadan	31	30	17.9
4	Federal University of Agriculture, Abeokuta.	23	21	12.6
5	University of Benin, Benin City	21	19	11.4
6	National Open University of Nigeria, Lagos	12	11	6.6
7	Federal University of Technology Akure	13	12	7.2
8	University of Ilorin, Ilorin	19	18	10.8
9	Federal University, Oye-Ekiti, Ekiti State	8	8	4.8
10	Federal University of Abuja, Abuja	7	7	4.2
Total		179	167	100.0

Table 2: Age of the respondents

Age	Frequency	Percentage (%)
18-25 years	2	1.2
26-35 years	62	37.1
36-45 years	86	51.5
46-55 years	6	3.6
56 years and above	11	6.6
Total	167	100.0

Table 3: Gender of the respondents

Sex	Frequency	Percentage (%)
Male	79	47.3
Female	88	52.7
Total	167	100.0

Table 4: Marital status of the respondents

Marital status	Frequency	Percentage (%)
Single	45	26.9
Married	122	73.1
Total	167	100.0

Table 5: Distribution of the respondents by highest educational qualification

Highest educational qualification	Frequency	Percentage (%)
Masters	125	74.9
M.Phil	23	13.8
PhD	19	11.4
Total	167	100.0

Table 5 shows that the highest number of respondents 125 (74.9%) had master degree certificates, 23(13.8%) had M.Phil certificate while, 19(11.4%) were PhD holders.

There are six research questions and one hypothesis formulated for this study in order to achieve the set objectives. Answers

to these research questions and hypothesis are provided below:

Research question 1: What is the level of awareness of cybersecurity among librarians in federal universities in South-West, Nigeria?

This question is answered with the data in Table 7.

Table 7: Level of awareness of cybersecurity among librarians

Awareness of cybersecurity I am aware of:	Very Highly Aware	Highly Aware	Aware	Not Aware	Mean	SD
Securing wireless networks on the computer	83(49.7%)	59(35.3%)	25(15.0%)	-	3.35	.727
Using ICTs in protecting privacy of information	40(24.0%)	72(43.1%)	55(32.9%)	-	2.91	.751
Protecting passwords used on computer	40(24.0%)	59(35.3%)	68(40.7%)	-	2.83	.789
Protecting e-mail account from hackers	7(4.2%)	21(12.6%)	91(54.5%)	48(28.7%)	1.92	.760
Protecting internet connected systems including hardware	7(4.2%)	5(3.0%)	103(61.7%)	52(31.1%)	1.80	.688
Keeping software and data from cyberattackers	7(4.2%)	-	94(56.3%)	66(39.5%)	1.69	.685
Overall mean					14.50	4.40

In order to determine the level of awareness of cybersecurity among librarians in federal universities in South-West, Nigeria, a test of norm was conducted. The scale between 0-8 shows that the level of awareness of cybersecurity among librarians is low, the scale between 9-17 indicates that the level of awareness of cybersecurity among librarians is moderate, and the scale between 18-26 shows that the level of awareness of cybersecurity among librarians is high. Thus, the overall mean for awareness of cybersecurity as indicated by the responses of the librarians is 14.5 which falls between the scales “9-17”. Therefore, it could be deduced that the level of awareness of cybersecurity among librarians in federal universities in South-West, Nigeria is moderate.

In particular, the awareness of cybersecurity among librarians in federal

universities in South-West, Nigeria with the highest means shows that librarians are aware of securing wireless networks on the computer (mean=3.35), and are also aware of using ICTs in protecting privacy of information (mean=2.91) respectively. This finding agreed with the findings of Symantec (2019) who stated that cybersecurity is the process of protecting and recovering networks, devices and programs from cyber-attack because cyberattacks are evolving danger to organisations, employees and consumers, designed an attack to access or destroy sensitive data or extort money, destroy businesses and damage people’s financial and personal lives. Rouse (2019) defines cybersecurity to be protection of internet connected systems including hardware, software and data from cyberattacks.

Research question 2: To what extent are librarians in federal universities in South-West, Nigeria aware of the potential cyber threats and attacks to library resources?

This question is answered with the data in Table 8.

Table 8: Extent librarians in universities in South-West, Nigeria are aware of the potential cyber threats and attacks to library resources

Extent of your awareness	Very High	High	Low	Very Low	Mean	SD
Destruction of information and other resources	112(67.1%)	3(1.8%)	52(31.1%)	-	3.36	.926
Interruption of services	33(19.8%)	82(49.1%)	51(30.5%)	1(0.6%)	2.88	.718
Data manipulation	29(17.4%)	43(25.7%)	94(56.3%)	1(0.6%)	2.60	.777
Delay in updating or dissemination of information	53(31.7%)	94(56.3%)	20(12.0%)	-	3.20	.633
Corruption or modification of information	67(40.1%)	54(32.3%)	46(27.5%)	-	3.13	.815
Loss of patron data or privacy ideas	53(31.7%)	92(55.1%)	22(13.2%)	-	3.19	.646
Overall Mean					18.36	4.515

In order to determine the extent librarians in federal universities in South-West, Nigeria are aware of the potential cyber threats and attacks to library resources, a test of norm was conducted. The scale between 0-8 shows that to a low extent are librarians aware of the potential cyber threats and attacks to library resources, the scale between 9-17 indicates that the extent librarians are aware of the potential cyber threats and attacks to library resources is moderate, and the scale between 18-26 shows that the extent librarians in federal universities in South-West, Nigeria are aware of the potential cyber threats and attacks to library resources is high. Thus, the overall mean for the extent librarians are aware of the potential cyber threats and attacks to library resources as indicated by the responses of the Librarians is 18.36 which falls between the scales “18-26”. Therefore, it could be deduced that the extent librarians in Federal universities in

South-West, Nigeria are aware of the potential cyber threats and attacks to library resources is high.

In particular, the extent librarians in federal universities in South-West, Nigeria are aware of the potential cyber threats and attacks to library resources with the highest means shows that librarians are aware of destruction of information and other resources (mean=3.36), are aware of delay in updating or dissemination of information (mean=3.20), and are also aware of loss of patron data or privacy ideas (mean=3.19) respectively. This finding corroborated the findings of Zhang and Bryant (2009) who explained that security perception and security practice to include usage of antivirus software, firewalls, passwords, email security habits and security education are important to users of internet. Kolb and Abdullah (2009), Paganini (2013) and Ray (2014) opined that educating employees through cybersecurity awareness programme

ultimately contributes to organisation's cybersecurity efforts and that employees risky online behaviour are responsible for many attacks, new business opportunities online, cloud and social media are privileged vectors to reach a wide audience unaware of cyber threats.

Research question 3: What is librarians' perception on the issue of cybercrime in university libraries in South-West Nigeria?

This question is answered with the data in Table 9.

Table 9: Librarians' perception on the issue of cybercrime in university libraries in South-West Nigeria

Items	Very just	Just	Unjust	Very unjust	Mean	SD
Having an unauthorized access to data and other computerized systems (hacking)	-	-	94(56.3%)	73(43.7%)	1.56	.498
Causing threats to library network	-	1(0.6%)	67(40.1%)	99(59.3%)	1.41	.506
Deliberate attack to destroy sensitive data in the library database	-	1(0.6%)	102(61.1%)	64(38.3%)	1.62	.498
Cyber-attacks to libraries to cause denied of access to users	-	1(0.6%)	74(44.3%)	92(55.1%)	1.46	.511
Use of the computer in committing crimes	-	1(0.6%)	100(59.9%)	66(39.5%)	1.61	.501

Table 9 presents results on the perception of the respondents on the issues associated with cybercrime, and results showed that most of the librarians (mean=1.62) noted that deliberate attack to destroy sensitive data in the library database is unjust. A significant number of the respondents (mean=1.61) affirmed that the use of the computer in committing crimes is unjust, while a notable number of the librarians (mean=1.56) also indicated that having an unauthorized access to data and other computerized systems (hacking) is considered unjust. This finding is in line with that of Newby (2014) who reported that libraries have made significant investment in computer based resources, training and services, however such investments need to be protected from abuse, misuse by taking active role in

cybersecurity. Also, Fischers (2016) gave the following as challenges of cybersecurity to be attack which compromise the confidentiality, integrity and availability of ICTs system, cyber theft or cyber espionage can result in exfiltration of financial, proprietary or personal information from which the attacker can benefit without knowledge of victim, denial of service can prevent legitimate users from accessing a system.

Research question 4: What are librarians' information technology skills to secure library resources?

This question is answered with the data in Table 10.

Table 10: Librarians' information technology skills to secure library resources

IT skills	SA	A	D	SD	Mean	SD
Hardware skill	73(43.7%)	69(41.3%)	12(7.2%)	13(7.8%)	3.21	.884
Software skill	54(32.3%)	75(44.9%)	38(22.8%)	-	3.10	.738
Operating system skills	39(23.4%)	94(56.3%)	34(20.4%)	-	3.03	.662
Content development software skills	53(31.7%)	57(34.1%)	57(34.1%)	-	2.98	.814
Programming language skills	33(19.8%)	102(61.1%)	32(19.2%)	-	3.01	.626
Database management system (DBMS)	12(7.2%)	130(77.8%)	25(15.0%)	-	2.92	.466

The study reveals librarians' information technology skills to secure library resources. Majority indicated that hardware skill (mean= 3.21), software skill (mean=3.10), operating system skills (mean=3.01), and programming language skills (mean=3.01) were the main librarians' information technology skills to secure library resources. This finding is in consonance with the findings of Usman and Gopakumar (2018) who opined that all library professionals have to acquire IT skills, mainly in three areas of information technology, i.e.

hardware, software and web applications. This is because electronic resources have become part of library resources. Therefore, management of electronic resources becomes the responsibility of librarian.

Research question 5: How do librarians in universities make use of both technical and non-technical security measures in libraries?

This question is answered with the data in Table 11.

Table 11: How librarians in universities make use of both technical and non-technical security measures in libraries

Items	SA	A	D	SD	Mean	SD
Technical security measures						
Access control and password security	43(25.7%)	124(74.3%)	-	-	3.26	.439
Video surveillance (CCTV system)	42(25.1%)	125(74.9%)	-	-	3.25	.435
Installation of updated software	43(25.7%)	100(59.9%)	24(14.4%)	-	3.11	.625
Run anti- virus software	23(13.8%)	77(46.1%)	67(40.1%)	-	2.74	.687
Malware scanners	22(13.2%)	94(56.3%)	30(18.0%)	21(12.6%)	2.70	.854
Non-technical security measures						
Architectural considerations	36(21.6%)	106(63.5%)	25(15.0%)	-	3.07	.603
Use of library personnel	30(18.0%)	113(67.7%)	2(1.2%)	22(13.2%)	2.90	.845

	%)	%)	%)			
Use of lighting protectors	30(18.0%)	109(65.3%)	28(16.8%)	-	3.01	.591
Burglary protection	30(18.0%)	134(80.2%)	3(1.8%)	-	3.16	.415
Fire extinguishers	30(18.0%)	133(79.6%)	4(2.4%)	-	3.16	.425

Table 11 shows that librarians make use of technical security measures in the libraries through access control and password security (mean=3.26), through video surveillance (CCTV system) (mean=3.25) and through installation of updated software (mean=3.11) respectively. While, the use of non-technical security measures in libraries by librarians are through burglary protection and fire extinguishers (mean=3.16 and mean=3.16); and architectural considerations (mean=3.07) respectively. This finding agreed with the findings of Singh and Margam (2018) who viewed Radio Frequency Identification (RFID), as considered to be the latest technology being used in libraries for self-checkout and check

in, book identification, sorting and conveying of library books and for theft detection. They further viewed that the Technological security refers to the security of library software, hardware, network security, server security, data security, workstations security and electronic security systems such as RFID, Fire alarms, Burglary protection and barcode, etc. (Singh and Margam, 2018)

Research question 6: What are the challenges encountered in securing information resources against cyberattacks?

This question is answered with the data in Table 12.

Table 12: Challenges encountered in securing information resources against cyberattacks

ITEMS	SA	A	D	SD	Mean	SD
Lack of trained information technology (IT) manpower	8(4.8%)	136(81.4%)	23(13.8%)	-	2.91	.423
People's negative attitude to change in technology	1(0.6%)	19(11.4%)	147(88.0%)	-	2.13	.350
Encountering technical problems in the course of usage	19(11.4%)	75(44.9%)	28(16.8%)	45(26.9%)	2.41	1.007
Crashing of a computer due to virus, malware, hackers etc.	21(12.6%)	125(74.9%)	20(12.0%)	1(0.6%)	2.99	.521
Lack of funds	43(25.7%)	71(42.5%)	53(31.7%)	-	2.94	.758

Table 12 shows that crashing of a computer due to virus, malware, hackers etc (mean=2.99), followed by lack of fund (mean=2.94) and followed by lack of trained information technology (IT) manpower (mean=2.91) were the main challenges

encountered in securing information resources against cyberattacks by librarians. This finding corroborated that finding of Ajie (2019) citing Davies (n.d) that cybersecurity measure is related to information security. Is a safety actions that

academic libraries can adopt for the installation of updated software, run anti-virus software, malware scanners, turn on firewalls protective barriers between computers and the internet, avoid spyware, protect passwords and back up important files to reduce risk of losing important information to virus, thefts and hackers.

Ho1: There is no significant relationship between awareness and perception of cybersecurity among librarians in federal universities in South-West, Nigeria.

The hypothesis is tested with data in Table 13.

Table 13: PPMC summary table showing correlation analysis between awareness and perception of cybersecurity among librarians in federal universities in South-West, Nigeria

Variables	N	Mean	Std.Dev	Df	R	P	Sig.
Awareness of cybersecurity	167	44.0479	5.45608	164	.048	.534	Not Sig.
Perception of cybersecurity	167	52.3413	12.57976				

Table 13 shows a low awareness of cybersecurity on perception of cybersecurity among librarians in federal university libraries (Df= 167, N= 164, $r = .048$, $P > .05$). Based on this, the null hypothesis is accepted. Therefore, there is no significant relationship between awareness and perception of cybersecurity among librarians in federal universities in South-West Nigeria. This finding is in line with the findings of Blackwood-Brown (2018) that cybersecurity awareness refers to educating internet users about cybersecurity issues, benefits, threats and attacks that can jeopardize their activities on the web, mitigate action against attack and how to prevent unauthorised users. Ray (2019) explains that users of internet should take the following precautions, installing anti-virus software, firewall, securing wireless networks and using spam filters.

Conclusion

Cybersecurity is an essential concept in library and information centres as information materials are prone to damages by unauthorised users known as cybercriminals. The activities of these unscrupulous elements are known as cybercrime. Academic libraries are experiencing various threats to resources.

This could be as a result of lack of trained information technology (IT) manpower in the library. Moreso, awareness of the librarians about cybersecurity is very important to combat the various threats to resources in their custody and provide adequate security to prevent unauthorised use and damage to library materials by cybercriminals.

In view of the conclusion drawn, the following recommendations are made:

1. The problem of crashing of a computer due to virus, malware, hackers etc. can be address by library management who are in the position of administration. They are to adequately monitor the information systems in the library with the help of the information system analyst by ensuring consistent update of computer, hardware and software and also monitor the activities of cyberhackers.
2. Government should provide adequate fund for universities to run their library effectively. Many universities experiences lack of fund to improve their library. Meanwhile, to provide appropriate security measures in libraries, there is a need of availability of funds.

3. The problem of lack of trained information technology (IT) manpower could be addressed by library management. library management should endeavour to enroll librarians for workshop on intensive IT training to be able to handle technical problems with the use of ICTs in the library.
4. There should be more awareness on issues with cybersecurity by library management. This is because awareness campaign will encourage readiness of the librarians to prepare against the activities of cybercriminals who infringed on authors right or causes damages to information materials.

References

- Adesina, O. S. (2017). Cybercrime and Poverty in Nigeria.” *Canadian Social Science Journal*, 13 (4).
- Ajie, I., (2019) A Review of Trends and Issues of Cybersecurity in Academic Libraries. *Library Philosophy and Practice*. <https://digitalcommons.unl.edu/libphilprac/2523>
- Blackwood-Brown, G. (2018). An Empirical Assessment of Senior Citizens’ Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills. https://nsuworks.nova.edu/gscis_etd/1047.
- Clough, J. (2014) Principles of Cybercrime. Cybersecurity issues and challenges: In brief. <https://a51.nl/sites/default/files/pdf/R43831.pdf>.
- Kerkhofs, J. (2018) Cybersecurity and Cybercrime, African Union Commission – Council of Europe Joint Programme. <https://au.int/en/pressreleases/20180412/africa-n-union-commission-and-council-europe-join-forces-cybersecurity>
- Kolb, N. & Abdullah F. (2009) Developing an information security awareness program for a non-profit organization. *International Management Review*, 5(2), 103.
- Ciampa, M. & Blankenship, R., (2019) Do Students and Instructors See Cybersecurity the Same? A Comparison of Perceptions about Selected Cybersecurity Topics”. *International Journal for Innovation Education and Research* 7 (1). Dhaka, Bangladesh: 121- 35. <https://doi.org/10.31686/ijer.vol7.iss1.1291>.
- Newby J., (2018) Information Security for Libraries <http://www.petascale.org/papers/librarysecurity.pdf>.
- Paganini, P. (2013). The impact of cybercrime.” *InfoSecInstitute*, 4(3),8 - 17. <http://resources.infosecinstitute.com/2013-impact-cybercrime/>.
- Mark R. (2014). Training Programs to Increase Cybersecurity Awareness and Compliance in Nonprofits <https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/19638/Ray2014.pdf>.
- Singh, V. & Madhusudhan M., (2018). Information Security Measures of Libraries of Central Universities of Delhi: A Study. *DESIDOC Journal of Library & Information Technology* 38(2).
- Symantec Internet Security Threat Report <http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed>.
- Koya, U. & Gopakumar V. (2018). Information technology skills required for library professionals in digital era: An introspection. *Information Technology*. 8 (1).
- Yalin, B. Eroğlu, & Başfirinci, S., (2019).

Cybersecurity Perceptions of University Students in Turkey. *Karadeniz Teknik Üniversitesi İletişim Araştırmaları Dergisi* 8(2) 2-14. <https://dergipark.org.tr/en/download/article-file/824317>.

Zhang, C. & Janet J., (2009). An empirical study of cyber security perceptions, awareness and practice. *Issues in Information System*, 1(2), 242-248. <https://iacis.org/iis/2009/P20091221.pdf>.