CURBING SECURITY THREATS IN ACADEMIC LIBRARIES: A SURVEY OF ACADEMIC LIBRARIANS' PERCEPTION ON CYBERCRIME AND CYBER SECURITY INFORMATION IN THREE SELECTED COLLEGES OF EDUCATION IN NIGERIA

Aji Kingsley Olawale[1] & Sule Yakubu[2]
[1] *FCT-Abuja*
[2] *Federal Capital Territory College of Education Zuba, Abuja*

E-mail: kingsola4u2003@gmail.com

Abstract

The study investigated academic librarians perception of cybercrime and cyber security information in curbing security threat in academic libraries in three (3) selected institutions namely; FCE, Zaria, FCT college of Education, zuba and Niger State College of Education, Minna. The study was guided by five (5) objectives and five (5) research questions. Descriptive survey research design was used for the study; the population is comprised of sixteen (16) academic Librarians in the three (3) selected colleges of education. Purposive sampling techniques was used for the study. Questionnaire was used as the data collection instruments while data collected were analyzed using descriptive statistics and results were presented in tables, frequency distribution, percentages and mean score. The findings of the study showed that; academic librarians perceived cybercrime as intellectual property theft, plagiarism, copyright violation, impersonation, software piracy among others. The findings from the study also revealed that academic librarians are aware of the following cybercrimes; cyber cracking, data breach, identity theft, cyber hacking, unauthorized access to information, copyright violation among others. It was also discovered that majority of the respondents indicated to a very high extent that the desire to get good grade, fear of failure, lack of good academic writing skills and desire to make money causes students involvement in cybercrime in academic libraries. The study further revealed lack of cyber security skills among academic librarian, poor password management, lack of cyber security infrastructure among others as challenges to the successful deployment of cyber security in academic libraries. The study suggests; cybercrime and cyber security awareness among academic librarians, library and internet literacy, deployment of cyber security infrastructure etc. as measures available to combat cybercrime in academic libraries.

Keywords: *Academic Libraries, Cybercrime, Cyber Security threat, Cyber Security, Colleges of Education*

Introduction

Academic libraries remains the bedrock for all research activities in academic institutions. The academic health, intellectual vitality and effectiveness of our academic institutions in producing high quality graduates into the labour market depends largely on the quality of information resources available in the library to support teaching, learning and research activities. Akinlubi (2015) defined academic libraries as libraries found in institutions of higher learning such as universities, polytechnics, colleges of education, school of nursing and other allied institutions. They are established to support teaching, learning and research process. Amidst the provision of information resources to support teaching, learning and research process, academic libraries also plays a pivotal role of providing protection and security for these information resources. Librarians are gate keepers in charge of the gate to knowledge. They are custodians as well as the gateway. As gatekeepers of information, they are trained to

disseminate information, or knowledge. They are also the ones to keep the gate, making sure nothing unauthorized goes out of the library and that whatever goes out is brought back in good condition (Oyelude and Bamigbola, 2012)

Today, the Internet and other information and communication technologies (ICTs) are pervasive in all of human endeavors. The demand for Internet and computer connectivity has led to the integration of these agents of change to everything and even other digital devices. The concept of Internet of things has taken the digital revolution further in the provision and use of this service. It has enabled the connection of computers to other digital devices and also to biological systems like the human beings. This fast development has not excluded the Library.

Cybercrimes are crimes and illegal activities perpetuated using electronic devices or computers via information systems and internet accessibility as its primary means of commission (Muktar, 2018). Cybercrime remains one of the biggest crimes perpetrated by youths in Nigeria. This crime is also known as "Yahoo-yahoo" in Nigeria (Geidam, 2023).

Studies on cybercrime has typically focused on the causes and effects of cybercrime in Nigeria (Adesina, 2017); laws penalizing against misuse of computer and have focused relatively on financial cost and socio-economic effects of cybercrime (Igba, Igba , Nwambam, Nnamani, Egbe & Ogodo, 2018). While these studies have helped to illuminate our understanding of cybercrime, the menace still persists at an alarming state.

In order to reduce the menace of cybercrimes as a threat to information systems security in libraries and the world at large, there is the need for a fresh perspective. Awareness and perception of cybercrimes by stakeholders that are supposed to be the capable guardians of these systems in the library is very essential (Muktar, 2018). This is critical because according to the Routine Activity theory(RAT), a crime occurs when there is the convergence of three elements; a motivated offender, a vulnerable target and the absence of a capable guardian (Yeboah, 2018). RAT theory is a criminological theory that was developed in the late 1970's by Marcus Felson and Lawrence Cohen. The theory suggests that crime occurs when three elements come together: A motivated offender, a suitable target, and the absence of a capable guardian. Crime in academic libraries occur when three element comes together (see Figure 1).

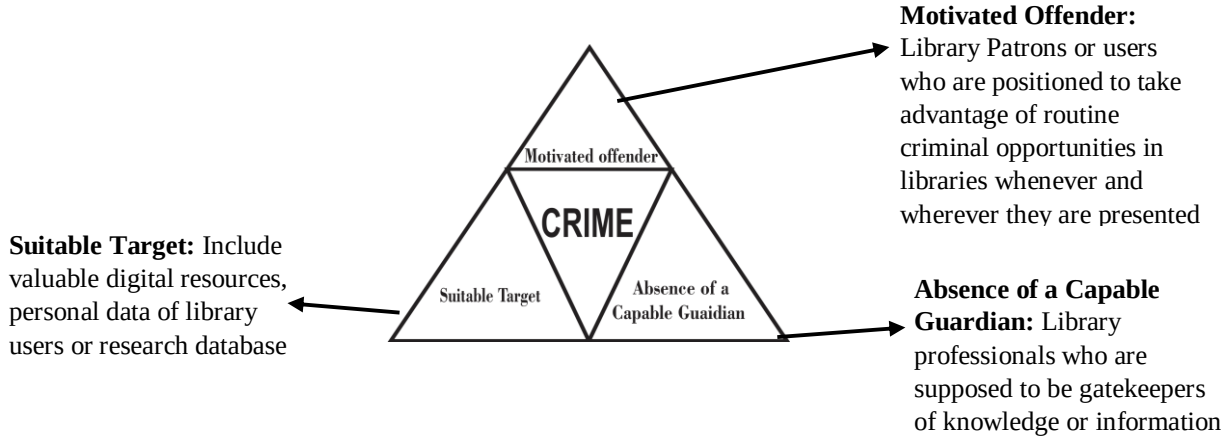

Figure 1: RAT theory Adapted from Cohen & Felson (1979)

Specifically, colleges of education in Nigeria are primarily set up to produce middle level man power for the basic schools in our educational system. The degree of academic excellence in

these schools is determined to a great extent by the quality of teachers produced at colleges of education. For effective learning and teaching in this set of institutions of higher learning therefore, a college library is fundamental. Academic libraries are libraries found in institutions of higher learning such as universities, polytechnics, colleges of education, school of nursing and other allied institutions. They are established to support teaching, learning and research process (Akinlubi,2015). Amidst the provision of information resources to support teaching, learning and research process, academic libraries also plays a pivotal role of providing protection and security for these information resources. In this regard, there is the compelling need to explore the Perception of cybercrime and cyber security information in curbing security threat in academic libraries in three (3) selected Colleges of Education in Nigeria

Problem statement

The contribution of the internet to the academic development of institutions of higher learning has been marred by the conscious evolution of new waves of crime. The internet has also become an environment where productive and safest offence thrives. One of the sources of free access to the Internet are the academic libraries in institutions of higher learning, while they provide these service to meet the educational demands of their users and to stay abreast with the digital revolution. Some users misuse these access by using the internet access provided and the integration of digital technologies by the libraries to perpetrate cybercrimes (Saulawa and Abubakar, 2014). Despite effort by the government to drastically reduce the activities of cyber criminals, cybercrimes are still on the rise, with newer scenarios coming out with every new case. It is difficult to estimate how many users of the internet are using it for illegal activities. According to Wall (2017) Cybercrime cannot be eradicated and there is no way to 'turn these technologies off'. However, cybercrime could only be managed in a way the risks and harm are reduced to the barest minimum. In order to reduce the prevalence of cybercrime in the country at large and in the college libraries in particular, there is the need to explore Academic Librarians' perception of cybercrime and cyber security information in curbing security threat in academic libraries in three selected Colleges of Education in Nigeria.

Objectives of the Study

The study determines the perception of Cybercrime and cyber security information in curbing security threats in academic libraries in FCE, Zaria, FCT college of Education, Zuba and Niger state college of education, Minna. However the specific objectives are to:

1. To find out how academic librarians in the three selected colleges of education perceive cybercrime.
2. To identify the types of cybercrime that academic librarians in the three selected colleges are aware of.
3. To ascertain the factors that cause students involvement in cybercrime in the three selected colleges.
4. To find out the challenges to the successful deployment of cyber security in academic libraries in the three selected colleges' education?
5. To find the measures put in place in curbing cybercrime by the academic libraries in the three selected colleges

Research Question

The following research questions will guide the study:

1. How do academic librarians in the three selected colleges perceive cybercrime?
2. What type of cybercrime are librarians in the three selected colleges are aware of?
3. What are the factors that cause students' involvement in cybercrime in the three selected colleges?

4. What are the challenges to the successful deployment of cyber security in academic libraries in the three selected colleges' education?
5. What are the measures put in place by academic libraries to curb cybercrime?

Literature Review

Crime and criminality have been associated with man since the fall. Nations across the globe have device various strategies to combat crime depending on their nature and extent. A nation with high incidence of crime cannot grow or develop. Globally, there are insecurity threats such as: Nuclear weapons, Climate Change, Terrorism, Energy,Peace and Conflicts, Poverty and Financial instability. While, in the academic library perspective, insecurity cuts across the following; library structural defects, network security, Cybercrime, Plagiarism, Piracy, Vandalism, Theft and Mutilation. We need an amplified international cooperation, which cannot be soft-hearted, but a realistic call to action that is demanded both domestically and internationally (Anuobia & Okoye, 2008). The internet can influence education and national development, and this has motivated academic libraries to establish electronic library (e-library) where users can readily access information from the internet. Opportunities of this nature are bound in universities and other higher institutions of learning in Nigeria in consonance with the goals of tertiary education which among others include: to acquire both physical and intellectual skills which will enable individuals to be self-reliance and useful members of the society (Igba, 2018). However, some people use these skills negatively and abuse this application of knowledge leading to criminality or cyber-crime

Igba etál (2020) carried out a study on cybercrime among university undergraduates: implications on their academic achievement. Three (3) objectives and three (3) research questions guided the researchers. Relevant literatures were reviewed in relation to the objectives. The study adopted descriptive survey research design. Questionnaire was used as the primary instrument for data collection. The population for the survey constituted of all the 891 undergraduates in FEDU, Ebonyi State University Abakaliki. The sample of the study comprised of 350 respondents. Purposeful sampling technique was used to select 50 undergraduates from each of the 7 departments chosen for the study for equal representation. Findings from the study revealed that the fear of unemployment had been the identity as a push factor for university undergraduates' involvement in cybercrime. The study also revealed that the possible strategies that could be employed to reduce the menace of cybercrime among university undergraduates involve the need to raise penalties and to increase the seriousness of offenders.

In a related study by Muhammad, Daniel & Samson (2020) on an empirical analysis of cybercrime trends and its impact on moral decadence among secondary school level students in Nigeria. The study adopted descriptive survey research design and was guided by 15 fact finding questions and the population of the study comprises of secondary school students within Kebbi and Sokoto State. Findings from study revealed among others that students within the age of 15-18(3) get mostly involve in online games and are the most victims of cybercrimes while students within the age of 10-14(1-2) are less victims since they seldom use mobile phones. However, the researchers discovered that, as their age advances their crime rates as well as victimization rate increases. Finally, the study also highlights ways to mitigate the worrisome growing rate of cybercrime carried out in some key sectors in Nigeria, especially the Secondary School institutions and presents a brief examination of these crimes in some secondary schools within Kebbi and Sokoto State, and proposed methods of cybercrime prevention to effectively combat cybercrime rate in the educational sector.

Abdulhamid, Haruna and Abubakar (2011) also conducted a study on "Cybercrimes and the Nigerian Academic Institution Networks". Two (2) objectives and two (2) research questions comprising of thirty two (32) items guided the researchers. Relevant literatures were reviewed in relation to the objectives. The study adopted descriptive survey research design. Questionnaire was used as the primary instrument for data collection. The population for the survey constituted students, Academic staff and non-academic staff in ten academic institions in Nigeria—two institutions in the north western region, five in the north-central region and three in the western region. The sample of the study comprised of 500 respondents. Out of the 500 questionnaires administered, 382 were found useful for the study. The study revealed that yahoo boy syndrome is more popular among students while Cyber plagiarism is more popular amongst lecturers. The study also revealed among others that cyber pornography and software piracy has a high rate of patronage in Nigerian academic institutions. The study also revealed that the possible strategies that could be employed to reduce the menace of cybercrime in Nigerian Academic institution involve the need to enact legislative laws that will specify punishments for all types of cybercrimes among others. But in the interim, academic institutions will have to devise their own ways of dealing with the perpetrators.

Muhammad, Daniel & Samson (2020) on an empirical analysis of cybercrime trends and its impact on moral decadence among secondary school level students in Nigeria. The study adopted descriptive survey research design and was guided by 15 fact finding questions and the population of the study comprises of secondary school students within Kebbi and Sokoto State. Findings from study revealed among others that students within the age of 15-18(3) get mostly involve in online games and are the most victims of cybercrimes while students within the age of 10-14(1-2) are less victims since they seldom use mobile phones. However, the researchers discovered that, as their age advances their crime rates as well as victimization rate increases. Finally, the study also highlights ways to mitigate the worrisome growing rate of cybercrime carried out in some key sectors in Nigeria, especially the Secondary School institutions and presents a brief examination of these crimes in some secondary schools within Kebbi and Sokoto State, and proposed methods of cybercrime prevention to effectively combat cybercrime rate in the educational sector.

Methodology

Descriptive survey research design was used for this study. The target population of the study were academic librarians in the three selected college of education in Nigeria i.e. Federal college of education, Zaria, FCT college of Education, Zuba and Niger state college of education, Minna. Purposive random sampling techniques was adopted for the study. This is because the three(3) selected colleges of education have fully implemented and embraced Information and Communication Technology in their library operations. The sample for the study was 16 respondents, mainly academic librarian from the three selected colleges of education. The instrument for data collection was a structured questionnaire tagged "Academic Library and Cybercrime Questionnaire (ALCCQ). The questionnaire had two sections A and B. Section A sought information on personal data of the respondents; Section B sought answers to research questions 1, 2, 3, 4 and 5 respectively. The items were structured on a Likert scale type. The questionnaire was subjected to face and content validation by experts in the field of Librarianship and information science. The internal consistency of the instrument was determined using Cronbach Alpha. The reliability coefficient of the instrument was α=0.98. The instrument was administered by the researcher through personal contact.

Result and Discussion

Data were analyzed with the use of descriptive statistics using frequency count, simple percentages, and mean score. A benchmark of 3.00 mean score was considered as accepted,

while below 3.00 was rejected. Out of the 16 questionnaire administered, 16 were duly filled and returned by the respondents. The rate of return was 100.0%.

Table 1: Distribution of respondents by Institution

Institutions	Frequency	Percentage
College of Education Minna	3	18.8
FCE, Zaria	5	31.2
College of Education Zuba	8	50.0
Total	**16**	**100.0**

Table 1 shows the distribution of respondents by institution. It shows that 3(18.8%) of the respondents are library academic staff of COE Minna while 5(31.2%) of the respondents are library academic staff of FCE, Zaria and 8(50.0%) library academic staff of COE Zuba. This shows that College of Education, Zuba has the highest number of library academic staff.

Table 2: Distribution of respondents by Gender

Sex	Frequency	Percentage (%)
MALE	11	68.8
FEMALE	5	31.2
Total	**16**	**100.0**

Table 2 shows the gender of respondents. It shows that 11(68.8%) of the respondents are male and 5(31.2%) of the respondents are female. This shows that there are more male than female academic staff in the three selected colleges of Education libraries.

Table 3: Distribution of respondents by Educational Qualification (Academic Librarian)

S/N	Qualification	Frequency	Percentage (%)
1	First Degree	6	37.5
2	Masters	9	56.3
3	Ph.D	1	1.7
	Total	**16**	**100.0**

Table 3 indicated that more than half 9(56.3%) of the respondents had Masters as their highest educational qualification, followed by 6(37.5%) with First degree, and only 1(1.7%) had Ph.D. This implies that majority of the respondents in the three selected colleges of Education libraries possess master's degree as their highest educational qualification.

Table 4: Distribution of respondents by Years of Working Experience

S/N	Years	Frequency	Percentage (%)
1	1-5 years	4	25.0
2	5-10 years	6	37.5
3	10-20 years	6	37.0

4	30 years & Above	0	0.0
	Total	**16**	**100.0**

Table 4 revealed that 6(37.5%) and 6(37.5%) of the respondents had between 5-10 years' and 10-20 years' experience as academic librarians, followed by 4(25%) with 1-5 years working experience as academic librarians.

Research Question One: How do academic librarian in colleges of education perceive

S/N	Perception of Academic Librarians on Cybercrime	VHE	HE	LE	VLE	$\bar{x}$	Decision
1	Academic librarians perceive cybercrime as intellectual property theft	12 (75.0%)	4(25.0%)	0(0.0%)	0(0.0%)	3.75	Accepted
2	Academic librarians perceive cybercrime as plagiarism	7(43.8 %)	9(56.3%)	0(0.0%)	0(0.0%)	3.44	Accepted
3	Academic librarians perceive cybercrime as copyright violation	10(62.5 %)	5(31.3%)	1(6.3%)	0(0.0%)	3.56	Accepted
4	Academic librarians perceive cybercrime as impersonation	10(62.5 %)	5(31.3%)	1(6.3%)	0(0.0%)	3.25	Accepted
5	Academic librarians perceive cybercrime as mailing fraudulent messages.	5(31.3 %)	9(56.3%)	1(6.3%)	1(6.3%)	3.13	Accepted
6	Academic librarians perceive cybercrime as unauthorized data access	6(37.5 %)	9(56.3%)	0(0.0%)	1(6.3%)	3.25	Accepted
7	Academic librarians perceive cybercrime as viewing naked pictures and nude videos.	3(18.8 %)	8(50.0%)	2(12.5%)	3(18.8%)	2.69	Rejected
8	Academic librarians perceive cybercrime as computer hacking.	10(62.5 %)	5(31.3%)	1(6.3%)	0(0.0%)	3.56	Accepted
9	Academic librarians perceive cybercrime as Piracy	7(43.8 %)	7(43.8%)	2(12.5%)	0(0.0%)	3.31	Accepted
10	Academic librarians perceive cybercrime as Internet Fraud	7(43.8 %)	8(50.0%)	1(6.3%)	0(0.0%)	3.38	Accepted
11	Academic librarians perceive cybercrime as diffusing false information about a person on social media/cyber bullying	6(37.5 %)	7(43.8%)	1(6.3%)	2(12.5%)	3.06	Accepted

Research Question Two: What type of cybercrime are academic librarians in college of education aware of?

The data that provided answer to the research question are presented in Table 6

Table 6: **Mean Rating of Respondents on Awareness of the Types of Cybercrime**

S/NO	Types of Cybercrime Academic Librarians are Aware of	SA	A	D	SD	$\bar{x}$	Decision
1	Cyber cracking	6(37.5 %)	6(37.5 %)	2(12.5 %)	2(12.5 %)	3.00	Accepted

2	Data breaches	4(25.0 %)	10(62.5 %)	2(12.5 %)	0(0.0%)	3.13	Accepted
3	Stealing of users email identity	4(25.0 %)	8(50.0 %)	4(25.0 %)	0(0.0%)	3.00	Rejected
4	Spyware or Identity theft	10(62.5 %)	6(37.5 %)	0(0.0%)	0(0.0%)	3.63	Accepted
5	Cyber hacking	7(43.8 %)	9(56.3 %)	0(0.0%)	0(0.0%)	3.44	Accepted
6	Unauthorized access to information	10(62.5 %)	5(31.3 %)	1(6.3%)	0(0.0%)	3.56	Accepted
7	Fraudulent Messages	5(31.3 %)	9(56.3 %)	2(12.5 %)	0(0.0%)	3.19	Accepted
8	Theft or breach of confidential information	8(50.0 %)	8(50.0 %)	0(0.0%)	0(0.0%)	3.50	Accepted
9	Computer virus infection	3(18.8 %)	6(37.5 %)	5(31.3 %)	2(12.5 %)	2.63	Rejected
10	Information forgery and counterfeiting	5(31.3 %)	9(56.3 %)	1(6.3%)	1(6.3%)	3.13	Accepted
11	Theft of hardware devices	2(12.5 %)	5(31.3 %)	5(31.3 %)	4(25.0 %)	2.31	Rejected
12	Impersonation	6(37.5 %)	9(56.3 %)	0(0.0%)	1(6.3%)	3.25	Accepted
13.	Plagiarism and copyright violation	9(56.3 %)	6(37.5 %)	0(0.0%)	1(6.3%)	3.44	Accepted

SA- Strongly Agreed **A-** Agreed **D-** Disagreed **SD-** Strongly Disagreed

From the result presented in Table 6 on research question 2 above, it was showed that the mean values of 10 out of the 13 items in the table ranged from 3.00 to 3.63 which are in each case greater than or equal to the cut-off point value of 3.00 on 4 point rating scale. This indicated that the respondents agreed that the 10 identified items i.e. cyber cracking, data breaches, spyware, cyber hacking, unauthorized access to information, fraudulent messages, Theft or breach of confidential information, information forgery and counterfeiting, impersonation, plagiarism and copyright violation are the types of cybercrime academic librarians are aware of. On the other hand, the mean values of item 3, 9 and 11 respectively which are in each case less than the cut-off point value of 3.00 on 4 point rating scale indicating that the three (3) items are not the types of cybercrime academic librarian are aware of.

Research Question Three: What are the factors that tend to cause students' involvement in cybercrime in colleges of education in Nigeria?

The data that provided answer to the research question are presented in Table 7

Table 7: **Mean Rating of factors that tend to cause students' involvement in cybercrime**

S/N	Factors that cause Students' involvement in Cybercrime in Academic Libraries	VHE	HE	LE	VLE	$\bar{x}$	Decision
1	The desire to get good grade and fear of failure lead undergraduate students to plagiarism.	8(50.0 %)	7(43.8 %)	1(6.3%)	0(0.0%)	3.44	Accepted
2	Lack of good academic writing skills.	10(62.5 %)	6(37.5 %)	0(0.0%)	0(0.0%)	3.63	Accepted
3	Internet make copy and paste easy is a major cause of plagiarism and copyright violation	6(37.5 %)	9(56.3 %)	0(0.0%)	1(6.3%)	3.25	Accepted

4	Most students now concentrate on how to make money than focusing on their academics	10(62.5 %)	6(37.5 %)	0(0.0%)	0(0.0%)	3.63	Accepted
5	undergraduates see internet fraud as a place to deploy their knowledge	7(43.8 %)	4(25.0 %)	2(12.5%)	3(18.8%)	2.94	Rejected
6	Cybercrime is viewed as social exposure	5(31.3 %)	5(31.3 %)	1(6.3%)	5(31.3%)	2.63	Rejected

VHE-Very High Extent **HE-** High Extent **LE-**Low Extent **VLE-**Low Extent

The analysis on Table 7 indicates that the mean values for items 1-4 are 3.44, 3.63, 3.25and3.63 respectively. This revealed that the mean values of 4 out of the 6 items in the table ranged from 3.00 to 3.63 which are in each case greater than the cut-off point value of 3.00 on 4 point rating scale. This indicated that the respondents agreed that the 4 identified items i.e. the desire to get good grade and fear of failure lead undergraduate students to plagiarism, Lack of good academic writing skills, Internet make copy and paste easy is a major cause of plagiarism and copyright violation, Most students now concentrate on how to make money than focusing on their academics and are the factors responsible for students' involvement in cybercrime in academic libraries. On the other hand, the mean values of item 5 and 6 which are in each case less than the cut-off point value of 3.00 on 4 point rating scale revealed that the items are not a factors responsible for students' involvement in cybercrime in academic libraries.

Research Question Four: What are the challenges to the successful deployment of cyber security in academic libraries in the three selected colleges' education?
The data that provided answer to the research question are presented in Table 8

Table 8: **Mean Rating of extent of the challenges to the successful deployment of cyber security in academic libraries in the three selected colleges' education?**

S/NO	Challenges to the Successful Deployment of Cyber Security in Academic Libraries	SA	A	D	SD	$\bar{x}$	Decision
1	Lack of cyber security skills among staff/ librarians	14(87.5%)	2(12.5%)	0(0.0%)	0(0.0%)	3.88	Accepted
2	Poor password management	4(25.0%)	11(68.8%)	1(6.3%)	0(0.0%)	3.19	Accepted
3	Lack of cyber security infrastructure	9(56.3%)	7(43.8%)	0(0.0%)	0(0.0%)	3.56	Accepted
4	Lack of cyber security measures and policy	5(31.3%)	11(68.8%)	0(0.0%)	0(0.0%)	3.31	Accepted
5	Inadequate funds to enforce cyber security	11(68.8%)	5(31.3%)	0(0.0%)	0(0.0%)	3.69	Accepted
6	Lack of interest/concern from library management	5(31.3%)	8(50.0%)	0(0.0%)	3(0.0%)	2.94	Rejected
7	Disregard for data privacy	6(37.5%)	10(62.5%)	0(0.0%)	0(0.0%)	3.38	Accepted
8	Vulnerability of cyber Security software	10(62.5%)	6(37.5%)	0(0.0%)	0(0.0%)	3.63	Accepted
9	Ignorance of cybercrime/cyber security information among stakeholders of the library	9(56.3%)	6(37.5%)	1(6.3%)	0(0.0%)	3.50	Accepted

SA- Strongly Agreed **A-** Agreed **D-** Disagreed **SD-** Strongly Disagreed

The analysis in Table 8 on research question 4 above revealed that the mean values of 8 out of the 9 items in the table ranged from 3.19 to 3.88 which are in each case greater than the cut-off

point value of 3.00 on 4 point rating scale. This indicated that the respondents agreed that the 8 identified items i.e. Lack of cyber security skills among staff/ librarians, Poor password management, Lack of cyber security infrastructure, Lack of cyber security measures and policy, Inadequate funds to enforce cyber security, Disregard for data privacy, Vulnerability of cyber Security software and Ignorance of cybercrime/cyber security information among stakeholders of the library are challenges to the successful deployment of cyber security in academic libraries. On the other hand, the mean value of item 6 which is less than the cut-off point value of 3.00 on 4 point rating scale indicate that the items is not a challenges to the successful deployment of cyber security in academic libraries.

Research Question Five: What measures are academic libraries putting in place to curb cybercrime?

The data that provided answer to the research question are presented in Table 9

Table 9: **Mean Rating of the Measures available to Combat Cybercrime/Cyber Threat in Academic Libraries**

S/NO	Measures available to Combat Cybercrime/Cyber Threat in Academic Libraries	SA	A	D	SD	$\bar{x}$	Decision
1	Cybercrime and Cyber security awareness	12(75.0%)	3(18.8%)	0(0.0%)	1(6.3%)	3.56	Accepted
2	Library and Internet literacy	5(31.3%)	10(62.5.0%)	0(0.0%)	1(6.3%)	3.19	Accepted
3	Access control	10(62.5.0%)	6(37.5%)	0(0.0%)	0(0.0%)	3.63	Accepted
4	Installation of CCTV cameras to check and monitor users activities	8(50.0%)	6(37.5%)	0(0.0%)	2(12.5%)	3.25	Accepted
5	Firewall protection to prevent outside attack	8(50.0%)	6(37.5%)	2(12.5%)	0(0.0%)	3.38	Accepted
6	Use of antivirus/malware software application to dispel hackers	8(50.0%)	8(50.0%)	0(0.0%)	0(0.0%)	3.50	Accepted
7	End-to-end encryption for communication devices	8(50.0%)	8(50.0%)	0(0.0%)	0(0.0%)	3.50	Accepted
8	Regular security software update	8(50.0%)	7(43.8%)	1(6.3%)	0(0.0%)	3.44	Accepted
9	Cybercrime policy/guidelines.	8(50.0%)	7(43.8%)	1(6.3%)	0(0.0%)	3.44	Accepted
10	Cyber security unit for quick response	7(43.8%)	8(50.0%)	1(6.3%)	0(0.0%)	3.38	Accepted
11	Avoid opening links on files which could be scamming you.	11(68.8%)	5(31.3%)	0(0.0%)	0(0.0%)	3.69	Accepted
12	Installation of computer systems with latest operating systems updater.	10(62.5.0%)	5(31.3%)	1(6.3%)	0(0.0%)	3.56	Accepted
13	Using strong password that cannot be easily guessed or captured by cyber-crimes.	11(68.8%)	5(31.3%)	0(0.0%)	0(0.0%)	3.69	Accepted
14	Avoid unnecessary disclosure of your	13(81.3%)	3(18.8%)	0(0.0%)	0(0.0%)	3.81	Accepted

	identity to unknown people.						
15	Wireless network must be password protected.	9(56.3%)	7(43.8%)	0(0.0%)	0(0.0%)	3.56	Accepted
16	Deployment of Radio Frequency Identification (RFID) in Academic Libraries.	8(50.0%)	7(43.8%)	1(6.3%)	0(0.0%)	3.44	Accepted

SA- Strongly Agreed **A-** Agreed **D-** Disagreed **SD-** Strongly Disagreed

The analysis on Table 9 indicates that the mean values for items 1-16 are above the cut-off point of 3.00 on 4 point rating scale. This revealed that the respondents agreed to all the statement i.e. Cybercrime and Cyber security awareness, Access control, Installation of CCTV cameras to check and monitor users activities, Library and Internet literacy, Firewall protection to prevent outside attack, Use of antivirus/malware software application to dispel hackers, End-to-end encryption for communication devices, Regular security software update, Cybercrime policy/guidelines, Cyber security unit for quick response, Avoid opening links on files which could be scamming you, Installation of computer systems with latest operating systems updater, Using strong password that cannot be easily guessed or captured by cyber-crimes, Avoid unnecessary disclosure of your identity to unknown people, Wireless network must be password protected and Deployment of Radio Frequency Identification (RFID) in Academic Libraries are Measures available to Combat Cybercrime/Cyber Threat in Academic Libraries

DISCUSSION OF FINDINGS

The study examined the perception of cybercrime and cyber security information in curbing security threat in selected colleges of Education libraries in Nigeria. The study revealed that academic librarians in colleges of education perceive cybercrime as intellectual property theft, plagiarism, copyright violation, impersonation, mailing fraudulent messages, unauthorized data access, computer hacking, internet fraud, piracy, cyber bullying, password stealing and cyber cracking. This is corroborated by Anuobia & Okoye (2008) where they opined that in academic library perspective, insecurity cuts across the following; library structural defects, network security, cybercrime, plagiarism, piracy, vandalism, theft and mutilation. In response to research question two(2), the study revealed that academic librarians in the three selected colleges of education are aware of the following cybercrimes; cyber cracking, data breach, identity theft, cyber hacking, unauthorized access to information, fraudulent messages, breach of confidential information, information forgery, plagiarism and copyright violation. This is supported by the study conducted by Abdulhamid, Haruna and Abubakar (2011) who found out that cyber pornography and software piracy, yahoo-yahoo boy syndrome and cyber plagiarism has a high rate of patronage in Nigerian academic institutions.

Response on research question three (3) on the factors that tend to cause students involvement in cybercrime in academic libraries revealed that the desire to get good grades, fear of failure, lack of good academic writing skills and the desire to make money causes students involvement in cybercrime in academic libraries. This is in agreement with the findings of Igba e'tal(2020) who posited that the fear of unemployment had been the identity as a push factor for university undergraduates' involvement in cybercrime. In response to research question four (4) the study revealed lack of cyber security skills among academic librarians, poor password management, lack of cyber security infrastructure, lack of cyber security measure and policy, inadequate fund to enforce cyber security, disregard for data privacy, vulnerability of cyber security software and ignorance of cybercrime/cyber security among stakeholder of the library as challenges to the successful deployment of cyber security in academic libraries in the three

selected colleges' education. Response to research question five (5) revealed that cybercrime and cyber security awareness, library and internet literacy, installation of CCTV cameras, Firewall protection, use of antivirus software, end to end encryption of communication devices, regular security software update, cybercrime policy guidelines, using strong password, deployment of Radio Frequency Identification among others in academic libraries are measures available to curb cybercrimes in academic libraries. This is supported by the study conducted by Abdulhamid, Haruna and Abubakar (2011) who found out that the possible strategies that could be employed to reduce the menace of cybercrime in Nigerian Academic institution involve the need to enact legislative laws that will specify punishments for all types of cybercrimes among others

SUMMARY OF MAJOR FINDINGS

Emanating from the research findings are the following;

1. The study revealed that academic librarians in college of education perceive cybercrime as intellectual property theft, plagiarism, copyright violation, impersonation, mailing fraudulent messages, unauthorized data access, computer hacking, internet fraud, piracy, cyber bullying, password stealing and cyber cracking
2. Findings from the study also revealed that academic librarians in the three selected colleges of education are aware of the following cybercrimes; cyber cracking, data breach, identity theft, cyber hacking, unauthorized access to information, fraudulent messages, breach of confidential information, information forgery, plagiarism and copyright violation.
3. The study further revealed that the desire to get good grades, fear of failure, lack of good academic writing skills and the desire to make money causes students involvement in cybercrime in academic libraries.
4. Majority of the respondents agreed that lack of cyber security skills among academic librarians, poor password management, lack of cyber security infrastructure, lack of cyber security measure and policy, inadequate fund to enforce cyber security, disregard for data privacy, vulnerability of cyber security software and ignorance of cybercrime/cyber security among stakeholder of the library as challenges to the successful deployment of cyber security in academic libraries in the three selected colleges' education
5. Majority of the respondents also agreed that cybercrime and cyber security awareness, library and internet literacy, installation of CCTV cameras, Firewall protection, use of antivirus software, end to end encryption of communication devices, regular security software update, cybercrime policy guidelines, using strong password and deployment of Radio Frequency Identification in academic libraries are measures available to curb cybercrimes in academic libraries.

CONCLUSION

The study examined the perception of cybercrime and cyber security information in curbing security threats in academic libraries using Federal College of Education, Zaria, FCT college of Education, Zuba and Niger State College of Education Minna as case study. The following conclusions were drawn based on the findings of the study. The results showed that academic librarians in the three selected colleges of Education have good knowledge on cybercrime and are aware of the types of cybercrime. They also believed that the desire to get good grades, fear of failure, lack of good academic writing skills and the desire to make money causes students involvement in cybercrime in academic libraries. Although majority of the academic librarians in the three selected colleges of Education agreed that lack of cyber security skills among academic librarians, poor password management, lack of cyber security infrastructure, lack of cyber security measure and policy, inadequate fund to enforce cyber security, disregard for data privacy, vulnerability of cyber security software and ignorance of cybercrime/cyber

security among stakeholder of the library as challenges to the successful deployment of cyber security in academic libraries. However some believed that lack of interest and concern from library management as constraint to the successful deployment of cyber security in academic libraries.

RECOMMENDATIONS

Based on the findings of the study, the following recommendations are proffered:

1. Academic libraries should secure their network information. When organization provides security for their networks, it becomes possible to enforce property rights laws and punishment for whoever interferes with their property.
2. Improving awareness and competence in information security and sharing of best practices among academic librarians through the development of a culture of Cyber security at all level in safeguarding the privacy rights of individuals when using electronic communications.
3. Written security policy should be placed on library notice boards and the college library Home page of Federal college of education, Zaria, FCT College of Education, Zuba and College of Education Minna for users' benefits.
4. Orientation of users and staff should be done regularly in the three academic libraries in
   order to impart user education into library users.
5. Staff training on how to prevent the culprits from Cybercrime within and outside the academic libraries.

Acknowledgement

The authors wish to thank Tertiary Education Trust Fund (TETFund) of Nigeria for their financial support in making this research work successful.

References

Abdulhamid, S.M., Haruna C. and Abubakar, A. (2011). Cybercrimes and the Nigerian Academic Institution Networks. The IUP Journal of Information Technology, 7(1), 51-57

Adesina, O.S. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science*, 13(4), 111

Adomi, E.,Igun, S. (2008). Combating Cybercrime in Nigeria. *The Electronic Library*, 26(5), 716-725

Aji, K.O.and Yakubu, S. (2023). Perception on Cybercrime Information in Curbing Security Threats in Academic Libraries in Two (2) Selected colleges of Educationin Nigeria. *International Journal of Library and Information Technology*, 3(1), 82-94http://www.gojamss.net/journal/index.php/IJLIT

Akinlubi, I.S. (2015). *Essentials of Library studies*. Oyo: Omo-Oje Publishers.

Anuobi, C.B, & Okoye, I.B. (2008). The role academic libraries in universal access to print and electronic resources in developing countries. *Library Philosophy and Practice*.Available at: http://unlib.unl.edu/LLP/anunobi-okoye.htm

Cohen, L.E. & Felson, M. (1979) Social Change and Crime Rate Trends: A Routine Activity

Approach, American Sociological Review, 44:588-608.
Geidam, A.A(2023, May, 9th). Cybercrime in Nigeria and its implication. Daily Trust
Halder, D. & Jaishankar, K. (2011). Cybercrime and the victimization of women: laws, rights,and regulations. Hershey, PA, USA: IGI Global.

Igba D.I, Igba E.C, Nwambam A.S, N namani, S.C, Egbe E.U. & Ogodo J. V.(2018).Cybercrime among University Undergraduates: Implications on their Academic Achievement. *International Journal of Applied Engineering Research,* 13(2), 1144-1154. http://www.ripublication.com

Latha, D. (2008). Jurisdiction Issues in Cybercrimes. *Law Weekly Journal*, 4, p. 86. Available at www.scconline.com (retrieved on August 29, 2019).

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

Muktar, B. (2018). Investigating Cybercriminals In Nigeria*:* A Comparative Study (Unpublished Ph.D Thesis) University of Salford, UK.

Oyelude, A.A. and Bamigbola, A.A. (2012). Libraries as the gate: "Ways" and "Keepers" in the knowledge environment. *Published in Hi-Tech News.* http://www.researchgate.net/publication/236331613

Saulawa,M.A. and Abubakar, M.K. (2014). Cybercrime in Nigeria: An overview of Cybercrime Act 2013. *Journal of Law, Policy and Globalization,* 32(1), 23-33.

UNODC (2013). Comprehensive Study on Cybercrime. Retrieved from http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_201213.pdf

Wall, D.S. (2017). Crime, Security and Information Communication Technologies: The Changing cyber security threat landscape and implications for regulation and policing, in R. Brownsword, E. Scotford and K. Yeung (eds). The Oxford Handbook on Law and Regulation of Technology, Oxford: Oxford University Press.

Yeboah, C. (2018). Cybercrimes-Technology's Menace of the 21st Century. Retrieved March 3rd 2022, from https://nrinews24x7.com/news_reg_cyber2015013105.html.