Assessment of Cybercrime Security Protocols and Challenges in Academic Libraries of Tertiary Institutions in Yobe State, Nigeria

[1]Augustine Alhaji Adejo, [2]Kabiru Akande Babatude & [3]Ajayi Joushua Eyiolorunshe

[1]Nigeria French Language Village, Ajara, Badagry, Lagos State, *adejoaugustine123@gmail.com*
[2]University Library, Federal University, Gashua, Yobe State, *kabiruakande@gmail.com*
[3]University Library, Federal University, Dutsin-ma, Katsina State ajayijoshua788@yahoo.com

Abstract:

The rapid integration of Information and Communication Technologies (ICTs) and internet connectivity in academic environments has exposed institutional libraries to persistent cyber threats, ranging from unauthorized access to data breaches. This study investigated the security measures adopted to control cybercrime and the challenges mitigating their effectiveness in three tertiary institutions (Federal Polytechnic Damaturu, Federal College of Education (Technical), Potiskum and Federal University, Gashua) in Yobe State. The study adopted a qualitative research method and a multiple case study design, data was collected through semi-structured interviews with 6 participants that were purposively selected as a sample from twenty (20) Staff of e-library/ICT staff and network administrators who frequently monitor clients who access online information from the three (3) tertiary Institutions with ICT/e-libraries and internet connectivity were considered as study participants. All the narratives from the 6 participants" were used for analysis. The data was analyzed using grounded theory Analysis. Findings revealed that while libraries employ fundamental security measures such as strong passwords, control software, and restricted network access keys, these protocols are currently ineffective against sophisticated cybercriminal tactics. Critical challenges mitigating the prevention cybercrime include lack of implemented cyber policies, inadequate technical expertise among staff, poor management attitudes, and insufficient funding for modern security infrastructure. The study concludes that the existing digital library environments are highly vulnerable to exploitation. It recommends the urgent development of a comprehensive cyber-security framework, the implementation of standardized cyber policies, and increased investment in specialized staff training and advanced security technologies, such as CCTV monitoring and system identification tracking, to ensure a secure and reliable digital research environment.

Keywords: Cybercrime, Academic Libraries, Cyber Security Protocols, ICT, Yobe State, Nigeria.

Introduction

Cybercrime has become a global phenomenon that emerges as a threat through Internet accessibility. cybercrimes are crimes committed through the use of World Wide Web (www) to steal someone's identity, watching and downloading of pornographic picture and films, spread of malicious software (virus), botnet (send spam email massages), accessing unwanted sites and hacking into other computer networks or websites (Babatunde, Muhammed and Aduku, 2019). Cybercrime has severe impacts on the society, ranging from its ability to aid corruption, money laundering, military espionage, terrorism and above all, undermining technological and socio-economic development of any country. Broadhurst & Chang, (2013) cited AFP, (2010) in their article that the United States Internet Crime Centre received 336,655 complaints reporting a total indirect losses of USD$559.7 million. According to Saulawa and Abubakar (2014), in 2012, an estimated $1 trillion was lost to cyber-related frauds globally. Although only $390 billion was reported for obvious reasons; and only recently a report by the South African based Institute of Digital Communication indicated that Nigeria is losing about $ 80 million dollars yearly to software piracy alone. Similarly, Sesan, Soremi&Oluwafemi (2012) reports that in 2012 alone, an estimated customer loss of ₦2,146,666,345,014.75 ($13,547,910,034.80) was incurred to cybercrime in Nigeria. Similarly, Folashade and Abimbola (2013) posits that cybercrime hinders the socio-economic development of the country as it endenders lack of trust and confidence in profitable transactions, promotes denial of innocent Nigerians opportunities abroad and causes loss of employment and revenue loss. Indeed, cybercrime also has an implication in the socio-economic advancement of the country as information flowing from the country is characterized as questionable, because of the criminal element that make it unreliable, inaccurate and untrustworthy, (Iwarimie-Jaja, 2010). Maitanmi, Ogunlere, Ayinde, &Adekunle (2013) findings show that cybercrime impedes socio-economic development in Nigeria as it scares away foreign investors due to the low level of confidence it has created for the Nigerian economy. The findings also show that cybercrime has aided other illicit activities in Nigeria such as intellectual plagiarism, disruption of public services, drug trafficking, and terrorism.

In addressing the impacts of cybercrime, Kamini (2011) argued that a nation with high incidence of crime cannot grow or develop; hence cybercrime leaves negative social and economic consequences. Furthermore, cyber security has now been elevated to the level of being handled by the Presidency through the Office of the National Security Adviser (ONSA). However, these could be seen in the presentation of the National Cyber Security Policy and Strategy drafts by the above-mentioned office. This has showed that national security is not restricted only to weapons and military preparedness but encompasses political, social and economic well-being of the people. In a nutshell, the Nigerian government has established cyber-security policy and strategy framework (Oluwafemi & Agada, 2015).

In May, 2015, the Cyber Crime Act came to force; the National Cyber Security Policy and Strategy drafts were officially presented at a symposium held in Lagos. Characterized by an unrestricted borderless nature, the importance of security policy implementation through standardized and functional strategies in securing cyberspace cannot be overemphasized because of the Nigerian Government commitment to achieve active support, participation and contributions of stakeholders from relevant sectors towards achieving increased national cyber security (Ogana, 2017). An attempt to address cyber-crime by various governments and international organizations has not been successful, owing to the fact that the identities remain inadequate (Okeshola & Adeta, 2013). Therefore, there is need for empirical study to be carried out in order to thoroughly assess cybercrime security protocol from various facets of human endeavour.

Statement of the Problem

The incorporation of ICTs and Internet connectivity at tertiary institutions in Yobe State has brought persistent challenges toward securing online platforms against unauthorized access and data breaches in respective institutions libraries. Despite the implementation of basic security protocols such as cautioning Internet users who login to other users account, viewing of classified and unwanted information, plugging of flash drive into computer system which may affect the system with viruses. And also blocking/suspending and denying users from login to the institution's network when found perpetrating unwanted act. Indeed, it has been observed that cybercriminals devise more sophisticated method to perpetrate crime. In addition, Oloyede et al. (2024), the "digital divide" in security infrastructure within African academic institutions often stems from a combination of management apathy and the absence of localized, enforceable cyber-laws, leaving sensitive research data and institutional networks at high risk of exploitation. However, could the vulnerability of academic libraries attributed to lack of implemented cyber policies, inadequate funding for modern security hardware and a deficiency in the technical expertise required to manage emergence threats.

Although, in order to achieve an effective cyber security in academic environment there is need to assess the available cyber security protocols and challenges mitigating the prevention of cybercrimes. This has prompted the researcher to in-depthly investigate the available cyber security as well as challenges encountered in preventing cybercrimes in academic libraries.

Objectives of the Study

The objectives of the study are:

1. To identify the security measures adopted to control cybercrimes in academic libraries in Yobe State
2. To examine the challenges encountered in preventing cybercrimes in academic libraries in Yobe State

Literature Review

The contribution of Internet to the development of the nation has been marred by the evolution of new waves of crime (Okeshola & Adeta, 2013). Cybercrime prevention is known as precaution steps to protect someone's technologies vulnerable to attacks. The term cyber prevention and cyber security are used interchangeably in this text. According to Kaspersky (2021), cybercrime security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories such as:

- ✓ **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- ✓ **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data that it's designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- ✓ **Information security** protects the integrity and privacy of both data and information in storage and transmission.
- ✓ **Operational security** includes the processes and decisions for handling and protecting data and information assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

- ✓ **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event.
- ✓ **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Every organization is taking cyber-security measures such as installing of anti-virus, management software, firewall, etc to prevent cybercrimes prevalence in their respective domain. In Nigeria Government has empowered the security agencies such as EFCC, NITDA, NCC, etc to arrest and prosecute cyber-crime culprits. In addition to this, cyber security has now been elevated to the level of being handled by the Presidency through the Office of the National Security Adviser (ONSA). However, these could be seen in the presentation of the National Cyber Security Policy and Strategy drafts by the above-mentioned office. This has shown that national security is not restricted to only weapons and military preparedness but encompasses political, social and economic well-being of the people. In a nutshell, the Nigerian government has established a cyber-security policy and strategy framework (Oluwafemi & Agada, 2015).

In May, 2015, the Cyber Crime Act came into force; the National Cyber Security Policy and Strategy drafts were officially presented at a symposium held in Lagos. Characterized by an unrestricted borderless nature, the importance of security policy implementation through standardized and functional strategies in securing cyberspace cannot be overemphasized because of the government commitment to achieve active support, participation and contributions of stakeholders from relevant sectors towards achieving increased national cyber security (Ogana, 2017).

Moreover, various studies were carried out on cybercrime prevention. Bandakkanavar (2019) indicated ways of tackling cybercrime such as using strong password, protect your identity online and protect your computer with security software. Moreover, password are frequently reset as well as ensuring that it is a strong password that comprises upper and lower alphabetical keys, including numerous, symbols, etc. in order to ensure cyber security. In this regard, Odumesi (2014) revealed that the uses of password are most common form of securing of network system. Mostly, all the systems are programmed to ask for username and password to access the computer system. Password should be changed after regular interval of time and should be alpha numeric and should be also difficult to judge. Indeed, using of software control system prevent unauthorized access to institutional network. Odumesi (2014) further indicated access control system using firewalls, which allow only authorized communications between internal and external networks and uses of firewalls, is beneficial to cybercrime prevention. Kratchman, Smith & Murphy (2008) study shows that the prevention measures include password, firewall, encryption and security policies and procedure.

Attempt to prevent cybercrimes prevalence end-up fruitless due to numerous challenges encountered by various organizations and individuals. In respect to this, Barfi, Nyagome &

Yeboah (2018), admitted that lack of frequent training on ICT, updating and amendment of cyber laws to cater for new offences under cybercrime is a challenge. They further stated that without such technical skills, new forms of cybercrime are more likely to go unnoticed and unpunished. Goodman & Brenner (2002) also indicated that cybercrime law are lacking in Africa, the Middle East, Asia and Oceania. Indeed, Chukwuma (2014) revealed that challenges of combating cybercrime include deficient legal framework, inadequate Cyberspace Security Capability (CSC) and insufficient Cyber Forensic Capacity (CFC).

- ✓ **Deficient Legal Framework**. There is presently no law that explicitly addresses cybercrime in Nigeria. Section 36(12) of the 1999 Constitution stated that an un-codified crime is not punishable. This implies that a cybercriminal can challenge his prosecution and go scot free. Therefore, deficient legal framework is a challenge to combating cybercrime for enhanced NSN.
- ✓ **Insufficient Cyber Forensic Capability**. The number of forensic investigators in Nigeria is negligible when compared to the number of cybercrimes committed in Nigeria. This stalls investigations and evidence analysis/case preparation. Thus, insufficient CFC is a challenge to combating cybercrime for enhanced NSN.
- ✓ **Inadequate Cyberspace Security Capacity**. Inadequate CSC makes Nigeria's cyberspace vulnerable to cyber-attacks. This occasioned where defacement of FGN websites has risen from 10 percent in 2010 to 60 percent in 2012.

Methodology

This study adopted the qualitative research method and multiple case study design. Twenty (20) Staff of e-library/ICT staff and network administrators who frequently monitor clients that access online information from the three (3) tertiary Institutions(Federal Polytechnic Damaturu, Federal College of Education (Technical), Potiskum and Federal University, Gashua) with ICT/e-libraries and internet connectivity were considered as study participants. Six (6) participants used as sample for this study were selected through purposive sampling technique. Semi-structured interview were used to source for data for this study. Tape recorders were used to record the interview which lasted for 30-45 minutes. The interview was analyzed using grounded theory Analysis.

Security measures adopted to control cybercrimes in Academic Libraries

The objective of this study sought to identify the security measures adopted to control cybercrimes in academic libraries in Yobe State. Three categories emerged from the narratives of the participants of this study namely; (1) Cyber security (2) Effectiveness of the cyber security (3) Proposed effective cyber security. The categories and their individual subcategories are depicted in Table 4.4 below;

Table 1: Security measures adopted to control cybercrimes in academic libraries

Research Objective	Categories	Subcategorie s
1. The security measures adopted to control cybercrimes in your Institution	1. Cyber security	1.1 Strong password 1.2 Controlled software

		1.3 Network security key 1.4 Granting access to authorize users only
	2. Effectiveness of the cyber security	2.1 Not effective
	3. Proposed effective cyber security	3.1 Installation of CCTV camera 3.2 Restrict movement to cyber room 3.3 Cyber policy 3.4 System identification number

Security Measures Adopted to Control Cybercrimes in Academic Libraries

The security measures adopted to control cybercrimes in academic libraries in Yobe State category describes the narratives related to how cybercrimes are controlled in academic libraries in Yobe State. It consists of four (4) sub categories: strong password, control software, network security key not easily obtained and granting access to authorized users only. These are explained below;

Strong password: This subcategory depicts narratives on information related to the ways cybercrimes are controlled in academic libraries in Yobe State. Participant 5 commented that;

"In order to prevent cybercrimes users are advised to frequently reset their passwords, and also uses strong password that comprise a combination of alphanumeric, upper and lower alphabetic, signs and symbols".

Software control: This sub-category also emerged from the narratives related to how cybercrimes were controlled in academic libraries of Yobe State. Participant 5 commented that, *"To prevent cybercrime, installation of management control software that moderate user's online activities are necessary".* However, participant 2 said, *"Network administrator must ensure that firewall is turn on to prevent malicious access into the school network".*

Network security key: This sub-category emerged from the way cybercrimes are controlled in academic libraries in Yobe State. Participant 1 stated that,

"I opined that the network security key of Wifi Protected Access (WPA) encrypts information that is exchanged between two or more connected devices should not be easy to obtain without proper authentication and verification to prove user's genuine registration and identity".

Granting access to authorized users only: This sub category is observed from the following narrative by Participant 4 thus, *"WPA should authenticate only authorized users to connect into the institution wireless network to exchange data with other devices on the institution's network".*

Ineffective cyber security

Ineffective cyber security category includes narratives related to how effective was cyber security in preventing cybercrimes in Academic Libraries in Yobe State. It consists of one (1) sub category: ineffective cyber security (4/32:12.5%). This is explained below:

Ineffective cyber security: This sub-category also equally emerged from the 6th participant narratives of this study. The participant stated that,
"It's not too effective because cyber criminals are still devising other means to commit crime on online platforms in the libraries. Therefore, the IT stakeholders are also trying to find means of tackling situation".

Proposed effective ways to prevent cybercrimes

The effective ways of preventing cybercrimes category includes narratives related to the views of an e-library staff and network administrators on the effective ways to prevent cybercrime on the online platforms in their institutions in Yobe State. It consists of four (4) sub categories: Installation of CCTV cameras, restrict movement to server room, cyber policy and system identification number. The individual subcategories are explained below:
Installation of CCTV camera**:** -This sub category is observed from the following narratives by participant 1,

"The ways to ensure effective means to prevent cybercrime is to install CCTV cameras all over e-libraries/ICT halls". Participant 4 puts it this way, *"with the installation of CCTV cameras the library staff could monitor all the activities going on in the library".* Participant 6 narrated that, *"The installation of CCTV cameras to monitor cyber user's movement will enhance appropriate control on cyber user's activities".*

Restrict movement to server room: This sub category is explained by Participant 3,

"I feel that movement should be restricted to server room". Participant 4 narrated that, *"people should be prevented from entering into the server room. It should strictly be out of bound for users except the staff of the department".*

Cyber policy: This subcategory depicts narrative on the effective ways to control cybercrime on in Academic Libraries in Yobe State. Participant 2 stated that,

"I think that if there is a lay down rules and regulations that will guide all internet users on online activities as well as caution users using the institution network and other IT gadgets. Indeed, the cyber policy (rules and regulations) will aid cyber security in the institution". Participant 6 says, *"My own view is that there should be a cyber-policy that all users must abide to".*

System identification number: This shows the narratives on proposed ways to control cybercrime in Academic Libraries of Yobe State. Participant 2 noted that,

"One of the most common ways to control cybercrime prevalence is through system identification number. However, with this number it will be very easy to know the user that makes use of a particular computer system to perpetrate crime". Participant 5 narrated that, *"You know that cyber criminals are very intelligent they will not want to leave any trace that could get them been caught. They prefer to use public computer systems. Therefore, with system identification number every*

registered user that utilizes the library system can be easily identified irrespective of place and time".

Challenges encountered in preventing cybercrime in Academic Libraries

This study sought to reveal the challenges encountered in preventing cybercrimes in academic libraries in Yobe State. Three categories emerged from the narratives of the participants of this study namely; (1) Factors that mitigate the prevention of cybercrimes (2) Factors that lead to the challenges of cybercrimes prevention (3) Resolution to the challenges that mitigate cybercrimes prevention. The categories and their individual subcategories are explained in Table 4.7 below;

Table 2: Challenges encountered in preventing cybercrime on online platforms
Sources: Interview

RQ	Categories	Subcategories
1. The challenges faced in preventing cybercrime in your Institution	1. challenges that mitigate cybercrime prevention	1.1 Lack of implementation of cyber policy 1.2 Technical-know-how
	2. Factors that lead to the challenges of cybercrime prevention	2.1 Lack of standard cyber policy 2.2 Management attitude 2.3 Poor funding
	3. Resolution to the challenges mitigating cybercrime prevention	3.1 Staff training 3.2 Adequate funding 3.3 Management support 3.4 Standard cyber policy

Challenges that Mitigate the Prevention of Cybercrime

The challenges that mitigate cybercrime prevention category include narratives related to the view of participants on the challenges mitigating the prevention of cybercrime on online platforms in their institutions in Yobe State. It consists of two sub categories: lack of implementation of cyber policy and technical-know-how. The individual subcategories are explained below:

***Lack of implementation of cyber policy*: -**This sub category is observed from the following narratives by participant 6 that, *"with all our effort to prevent cybercrime we have not been given the privilege to implement the proposed cyber policy".* Participant 2 stated that, *"we have try all* *our possible best to draft rules and regulations that we hope will aid to prevent cybercrime but we have not been authorized to implement it".*

Technical knowhow: This sub category is derived from narratives related to the challenges that mitigate cybercrime prevention on online platforms. Participant 4 revealed that, *"one of the challenges we face in preventing cybercrime is that some of our staff are not knowledgeable enough on IT appliance*

Factors that lead to the challenges of cybercrime prevention

Factors that lead to these challenges that mitigate cybercrime prevention category include narratives related to the factors that lead to the challenges that mitigate cybercrime prevention were derived from the participants in academic libraries in Yobe State. It consists of three subcategories namely; lack of standard cyber policy, management attitude and poor funding.

Lack of standard cyber policy: sub-category emerged from the narratives related to the factors that lead to the challenges that mitigate cybercrime prevention in academic libraries in Yobe State. Participant 2 noted that,

"Lack of standard policy on cybercrime slows the processes in addressing cybercrime issues. However, the available policy cannot thoroughly redress cybercrime".

Management attitude: sub-category narratives were derived from participant 3, who stated that,

"The management attitude toward cyber security and prevention is very poor. In most cases, we send request letter seeking for approval for necessary items that will aids in controlling of cybercrime but it ends up fruitless". Participant 5 narrated this, "*When we present issues to the management they show less concern".*

Poor funding: Sub-category narratives emerged from participant 5 that,

"Adequate funding was not provided for us to procure some necessary items such as software packages, physical hardware and other useful materials and services that will aid cyber security issues and activities".

Resolution to the challenges mitigating cybercrimes prevention

Resolution to the challenges mitigating cybercrimes prevention category includes narratives related to the resolution of the challenges mitigating the prevention of cybercrimes in academic libraries in Yobe State. It consists of four subcategories namely; staff training, Adequate funding, management support and cyber policy. The individual subcategories are explained below:

Staff training: This sub-category was uncovered from the narratives related to the resolution of the challenges mitigating the prevention of cybercrime in academic libraries in Yobe State. Participant 4 said that,*" in order to improve cyber security there is need to engage the staff at the e-Library/ICT unit or department to undergo training".* In the same manner participant 7 says, *"Staff should be sponsored to undergo IT related programs, workshop and seminars".* Participant 1 remarked that, *"I will suggest that staff should be given the privilege to undergo training on crime related issues with IT appliance".*

Adequate funding: This sub category was derived from inclusive narrative related on the views on how to address the challenges that mitigate cybercrime prevention in Academic Libraries in Yobe State. Participant 5 narrated that, "*fund should be provided at due time in order to procure* *necessary equipment and materials needed".* Participant 6 summed up by saying that, *"according to my own view, I suggest that fund should always be available mostly when the need arises".*

Management support: This sub category was derived from participant 6 who narrated that, "*To me, the major way to address these challenges is that the management should show concern and ready to turn a listening ear on the overall activities going on in the library/ICT department".* Participant 1 stated that, *"management should always ensure that crime related issues are thoroughly investigated and also ensure that they deal with cyber culprits".*

Cyber policy: This subcategory also emerged from narratives on participant's views on how to address the challenges that mitigate cybercrime prevention. Participant 2 said, *"One of the easiest ways to address these challenges mitigating cyber security and prevention is to make provision for effective cyber policy that will serve as rules and regulations to guide internet users".* Participant 4 revealed that, *"The best way to address these challenges is for the stakeholders to come together and enact standard cyber policy and ensure that it be implemented".*

Security Measures Adopted to Control Cybercrimes in Academic Libraries

Three findings derived from responses of participants on the question about the security measures put in place to control cybercrimes in academic libraries in Yobe State. The cyber security measures adopted to control cybercrimes are through the use of strong password, control software, strictness to obtain network security key and granting access to authorized users only. This agrees with the study of Kratchman, Smith & Murphy (2008), study shows that the preventive measures including password, firewall, encryption and security policies and procedures. Bandakkanavar (2019) indicated ways of tackling cybercrime as using of strong passwords, protection of online identity and protection of computer with security software. Moreover, passwords are frequently reset to ensure strong passwording (that comprises upper and lower alphabetical keys and numbers, symbols etc.). Related to this, Odumesi (2014) revealed that use of password is the most common way of securing system network. Mostly, all the systems are programmed to ask for username and password before granting access to the computer system. Password should be changed at regular intervals of time and should be alpha numeric and difficult to guess. Indeed, using software control system prevents unauthorized access to institutional network. Odumesi (2014) further indicated that access control that allows only authorized communications between internal and external network and use of firewalls aid cybercrime prevention.

However, this study showed that the available cyber security is ineffective to effectively address cybercrime prevalence in the institutions. This is in line with the findings of Kratchman, Smith & Murphy (2008) that indicated that preventive techniques on cybercrime are fallible. This study further proposed effective ways to prevent cybercrimes such as installation of CCTV camera, restrict movement to server room, cyber policy and through system identification number. However, this finding agreed with Okeshola & Adeta's (2013) study that recommended immediate enactment of a comprehensive law on cybercrime to redress cybercrimes prevalence. The implication of this finding is that available cyber security measures cannot prevent cybercrime prevalence in academic libraries. Therefore, there is need to devise an effective cyber security and prevention that will effectively redress cybercrimes perpetration in academic libraries in Yobe State.

Challenges Encountered in Preventing Cybercrime in Academic Libraries

This study setting indicated that the challenges that mitigate cybercrime prevention are lack of implementation of cyber policy and poor technical-know-how. In Barfi, Nyagome & Yeboah (2018), findings admitted lack of frequent training on ICT, updating and amendment of cyber laws to cater for new offences under cybercrime is a challenge. However, they further stated that without such technical skills, new forms of crime were more likely to go unnoticed and unpunished. Goodman & Brenner (2002), also indicated that cybercrime law were lacking in Africa, the Middle East, Asia and Oceania

Moreover, those factors that lead to these challenges that mitigate cybercrime prevention are lack of standard cyber policy, management attitude and poor funding. In this study, the proposed resolutions to the challenges mitigating cybercrime prevention are training of staff, adequate funding, cyber policy and management support. The implication of these cyber challenges will enable cybercrime prevalence's in Academic Libraries. Thus, cyber security can be achieved through management support, provision of adequate funding and staff training.

Conclusion

The fundamental security measures adopted in academic libraries of tertiary institutions in Yobe State such as strong passwords, control software, and restricted access are currently ineffective against the rising tide of cybercrime. The findings highlight a significant gap between existing security efforts and the practical realities of cyber threats, primarily driven by poor management attitude, lack of standard cyber policies, and insufficient funding. Therefore, the findings proffer toward more advanced measures such as CCTV monitoring, system identification tracking, and that specialized staff training should be integrated in the existent security measure in order to ensure reliable digital library environment.

Recommendations

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

There is need for the Management of Federal University,Gashua, Federal Polytechnic, Damaturu and Federal College of Education (Technical), Potiskum in conjunction with cyber security experts to use the identified cyber-security measures to develop a cyber-security framework that would effectively prevent cybercrimes on libraries network.

There is need for the Management of Federal University, Gashua, Federal Polytechnic, Damaturu and Federal College of Education (Technical), Potiskum to act fast to resolute the challenges mitigating cyber prevention through implementation of cyber policy, training of staff (cyber security experts) and notifying security agencies on the nature cybercrimes in their institution in order to arrest and punish cyberspace offenders.

References

Babatunde, K. A., Muhammd, Y. A., & Aduku, S. B. (2019). Assessment of cyber and Social Media Crimes in the Library and ICT Unit of the Federal University, Gashua, Nigeria. *Journal of Environment, Technology & Sustainable Agriculture*, 1(1), 45-51.

Bandakkanavar, R. (2019). Causes of Cyber Crime and Preventive Measures. Krazytech; Retrieved on 16/9/2021, Available at: https://digitalpolice.gov.in

Barfi, K. A., Nyagorme, P. &Yeboah, N. (2018). The Internet Users and Cybercrime in Ghana: Evidencefrom Senior High School in BrongAhafo region. *Library Philosophy and Practice (e-journal)*, Retrieved on 12/6/2021, available at; https://digitalcommons.unl.edu/libphilprac

Broadhurst, R. &Chang , L. Y.C. (2013). Cybercrime in Asia: Trends and challenges. Handbook of Asian Criminology, Vol. 4 p. 49-63. Available at: DOI 10.1007/978-1-4614-5218 8_4,

Chukwuma, S. N. (2014). Cybercrime and National Security in Nigeria: Issues and Challenges. https://www.academia.edu/17211242/Cybercrime_and_national_security

Folashade B.O and Abimbola K.A (2013): The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International *Journal of Contemporary Research*. Vol. 3 No. 9; September 2013

Goodman, M. D., and Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, 10(2) 139-255. Available at: https://doi.org/10.1177/0190272513518337

Iwarimie-Jaja D. (2010): Criminology, Crime and Delinquency in Nigeria. Port Harcourt, Pearl Publishers.

Kamini, D. (2011). Cyber Crime in the Society: Problems and Preventions. *Journal of Alternative Perspectives in the Social Sciences*, 3(1), 240-259

Kaspersky, (2021). What is Cyber Security? Available at: www.kaspersky.com/resource center/definitions/what-is-cyber-security. Retrieved on 6/2/2021.

Kratchman, S., Smith, J. L., & Smith, M. (2008). The Perpetration and Prevention of Cybercrimes. Available at SSRN 1123743.

Maitanmi O., Ogunlere S, Ayinde S, & Adekunle Y. (2013): Impact of Cybercrimes on Nigerian Economy. *The International Journal of Engineering And Science (IJES)*, Volume 2, Issue 4, Pages 45-51

Odumesi, J. O. (2014). Combating the Menace of Cybercrime. *International Journal of Computer Science and Mobile Computing*, 3(6), 980-991. Retrieved from 23/06/2020; Available Online at: www.ijcsmc.com

Okeshola, F. B. & Adeta, A. K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, 3(9), p. 98-114.

Oluwafemi, O. & Agada, D. O., (2015). National Cyber Security and Strategy of Nigeria: A Qualittive Analysis. *International Journal of Cyber Criminalogy (IJCC)*, 9(1), p.120-144. Available at: https://zenodo.org/record/22390#.Y5P9gsvTXqA

Oloyede, M. O., et al. (2024). Digital Vulnerabilities in Higher Education: An Analysis of Cyber security Posture in West African Universities. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 14(1), 22-40.

Saulawa, M. A., & Abubakar, M. K., (2014). Cybercrime in Nigeria: An Overview of Cybercrime Art 2013. *Journal of law, Policy and Globalization*, Vol. 32, p. 23-33. Available at: www.iiste.org/Journals/index.php/JLPG/article/view/18571/18708

Sesan G., Soremi B., & Oluwafemi B. (2013): Economic Cost of Cybercrime in Nigeria. Cyber Steward Network Project of the Citizen Lab. University of Toronto.