

Combating Cybercrimes in Federal University Digital Libraries in Nigeria

Okoye, M.O. and Osadebe, N.E.

University of Nigeria, Nsukka

Enugu State, Nigeria.

Abstract

This study was focused on cybercrimes existing in Federal University Digital Libraries. Questionnaire was used for data collection from 120 librarians working in Federal University Digital Libraries in Nigeria. A survey research design was used for the study. The population of the study was made up of 120 librarians. Mean and percentages were used for data analysis. The major findings include that internet pornography and scam mails were the greatest cybercrimes committed in Federal University Libraries. It also identified major stakeholders in the control of cybercrimes as staff in charge of the computer systems. It was further revealed that non-coverage of cybercrimes under library laws and regulations constituted critical challenge to the control of cybercrimes. The study recommended among others, the need to entrench stiff penalties against cybercrimes in University laws and regulations so as to instill discipline and sustain relevance of cybercafés in enhancing academic excellence.

Key words: Universities, Academic Libraries, Cybercrimes, Digital Libraries, Stakeholders and Cybercrime control.

Introduction

Many forms of cybercrime exist. Asokhia (2010) notes that cybercrime covers a wide range of illegal activities including financial scam, computer hacking, downloading of pornographic images and virus attack to mention but a few. He further notes that recently young students in tertiary institutions engage in forgery of all kinds ranging from false admission papers to school fees' receipts, certificate racketeering and examination malpractice. Laumbano and Nawe (2004) reported that students in Dar es Salaam University, Tanzania used the internet

to view pornography. Ewuuk and Shannon (2009) also note that data theft and malicious break-ins are prevalent among students in Nigerian Universities. Rathinasabapathy and Rajendran (2007) called on library and information professionals especially those working in academic libraries to ensure enough safety and security of their data bases. It has been established by authors such as Longe and Chiemeké (2008) as well as Asokhia (2010) that youths between the ages of 15-30years are the major culprits of cybercrimes. Hence the developmental stage of adolescents that would have been used

to inculcate positive values is spent in cybercrimes to the detriment and the future of the Nigerian state. Boateng et al. (2010) argue that from the perspective of Information and Communication Technology (ICT) for development, that cybercrime has the potential to stall developmental contributions accruable from a well harnessed ICT adoption, diffusion and use. They also argue that cybercrime has the potential to widen the digital divide and affect consumer confidence in online transactions. Cybercriminals capitalize on system vulnerabilities, ignorance and gullibility on the part of users, to perpetrate their crimes. Boateng et al. (2010) noted that financial losses occasioned by cybercrime in the United States of America increased dramatically from \$52.5 million in 2006 to \$67 million in 2007.

Cybercrime is one of the fastest growing criminal activities in the world among youths. Padhye and Gujar (2012) observe that the total global economic loss due to cybercrime annually, is estimated at \$388 billion, out of which 114 billion is a result of direct losses in money stolen by cyber tugs and \$274 billion losses are due to time lost in dealing with cybercriminals. In 2008, the Internet Crime Report of the National White Collar Crime Centre ranked Nigeria 3rd in the world and 1st in the African Continent, as the source of fraudulent cyber activities. (National White Collar Crime Centre, 2008). Akuta, Ong'oa and Jones (2011) included Nigeria as one of the countries that served as cybercrime capital of the world. In a bid to control cybercrimes,

bodies such as International Police (INTERPOL) and the International Crime Commission have been instituted. The Nigerian Government has set up a number of commissions to combat cybercrime in Nigeria. According to Ehimen and Bola (2010) such commissions include: the Economic and Financial Crime Commission (EFCC) which was established in 2003, the Nigerian Cyber Working Group (NCWA), The Critical Information Infrastructure Protection Bill of 2005 and the Advance Fee Fraud act of 2006. Unfortunately, none of these organs has an office in any Nigerian University. Individually, some commercial and government owned cybercafés install Content Filter software in their computer systems to filter unwanted internet contents such as unsolicited messages. Notices, warning against spamming activities adorn the walls and notice boards of some organizations (Longe and Chiemeké, 2008). Also Curry, Flodin and Matheson (2000) suggested the use of security personnel within libraries to forestall cybercriminal activities.

The challenges of controlling cybercrime are daunting. Longe and Chiemeké (2008) observed that the crime came into existence with the recent emergence of cyber space. This explains the unpreparedness of the global society towards combating them. Boateng et al. (2011) observe that the laws of some nations and institutions (which include libraries) do not cover cybercrime. Wada and Odulaja (2012) posit that presently, there is no law specific to cybercrime in Nigeria.

Cybercrime often involves more than citizens of a nation. This means that to enforce control could demand international cooperation. Unfortunately, cybercrime knows no boundaries, a fact that complicates its investigation.

The evolution of fixed wireless facilities in the Nigerian network landscapes has added another dimension to the cybercrime problem. Longe and Chiemeké (2008) noted that fraudsters, who could afford internet connectivity through fixed wireless lines, operated through the comfort of their homes. Available reports on cybercrime and criminology in Nigeria by several authors including Longe and Chiemeké (2008) Ehimen and Bola (2010), Asokhia (2010) dwelt on cybercrime and criminality in Nigeria, cybercrime in Nigeria; and cybercrime and national development in Nigeria. None of these works or any other, to the best knowledge of the researchers targeted Federal University Digital Libraries. It is in this connection coupled with unfettered spread and unwholesome effects cybercrimes are visiting on society, that this study has been undertaken to fill the gap of finding a panacea to curb the nefarious crimes in Nigerian Federal Universities. In this study, cybercafés and digital libraries were used interchangeably.

Objectives of the Study

The general objective of this study was to examine ways through which Federal University Digital Libraries in Nigeria were combating cybercrimes. Specifically the study

1. Identified forms of cybercrimes that exist in the Federal University Digital Libraries in Nigeria
2. Identified stakeholders involved in controlling cybercrimes in Federal University Digital Libraries in Nigeria.
3. determined strategies used in controlling cybercrimes in Federal University Digital Libraries in Nigeria.
4. determined challenges of controlling cybercrimes in Federal University Digital Libraries in Nigeria.

Research Questions

The following research questions guided the study.

1. What forms of cybercrime exist in Nigerian Federal Universities?
2. Who are the stakeholders in controlling cybercrime in Nigerian federal Universities?
3. What are the challenges of controlling cybercrime in the University Digital Libraries?
4. What are the strategies employed by these Universities in controlling cybercrimes?

Methodology

Design and Area of Study: The study was a descriptive survey. The area of the study is Nigeria.

Population for the Study: Population for the study comprised all the twenty-four Federal Universities listed in Association of Commonwealth Universities (2008). The total population of academic librarians in the twenty-four Federal Universities was 120. All the 120 academic librarians were used

for the study because of the small size of the population. There was no sampling *Instrument for Data Collection*: A well structured questionnaire was used for data collection. It was developed through literature review based on the purpose of study. The reliability of the questionnaire was established using Cronbach's alpha formula. It was found to be 0.76. The questionnaire had two sections, sections A and B. Section A was based on respondents' demographic information while section B was based on aspects of cybercrime. Section B had four clusters. Clusters one and two were based on no or yes answer while clusters three and four were based on a four point scale of SA=Strongly Agree; A= Agree; D=Disagree and SD= Strongly Disagree.

Data collection and analysis techniques: One hundred and twenty copies of the questionnaire were administered to librarians working in library cybercafés. The 2012 Nigerian Library Association Annual General Conference held in Abuja offered researchers the opportunity to meet the respondents. During pre-conference lecture, announcements were made in which

librarians working in library cybercafés were asked to wait at the Eastern door of the conference room. The researchers addressed the librarians there and appealed to them to help make the research a success by filling copies of the questionnaire. Of the 120 copies of the administered questionnaire, 105 were completely filled and returned. All the 105 copies of the questionnaire were found usable. The 105 copies of the questionnaire were sorted into 6 geopolitical zones of the country. Percentages and mean scores were used for data analysis. Percentages of 50 and above were upheld. Also mean scores of 2.5 and above were upheld.

Findings

Characteristics of respondents

All the respondents had MLS as their highest library qualification. It also showed that sixty-six librarians (62.86%) and thirty-nine librarians (37.14%) had 1-5 years and 6-10 years professional experience respectively. Sixty librarians (57.14% and forty-five librarians (42.86%) were librarian 11 and librarian 1 respectively.

Types of cybercrimes

Table 1. Percentage Response on types of Cybercrime Existing in Nigerian Federal University Digital Libraries. N=105

Types of Cybercrimes	Geopolitical Zones in Nigeria						Total	%	D
	N.W	N.E.	N.C.	S.S.	S.W.	S.E.			
1 Scam mails	13 (12.38%)	9 (8.57%)	28 (26.67%)	15 (14.29%)	14 (13.33%)	18 (17.14%)	97	92.38	U
2 Internet Pornography	13 (12.38%)	10 (9.52%)	27 (25.71%)	17 (16.19%)	12 (11.43%)	19 (18.10%)	98	93.33	U
3 Data Interception	9 (8.57%)	6 (5.71%)	15 (14.29%)	12 (11.43%)	8 (7.62%)	12 (11.43%)	62	59.05	U
4 Data Modification	8 (7.62%)	7 (6.67%)	17 (16.19%)	14 (13.33%)	9 (8.57%)	15 (14.29%)	70	66.67	U
5 Data Theft	13 (12.38%)	10 (9.52%)	21 (20.00%)	17 (16.19%)	9 (8.57%)	16 (15.24%)	86	81.90	U

6	Network Sabotage	11 (10.48%)	6 (5.71%)	17 (16.19%)	12 (11.43%)	6 (5.71%)	14 (13.33%)	66	62.85	U
7	Unauthorized access	10 (9.52%)	8 (7.62%)	17 (16.19%)	13 (12.38%)	9 (8.57%)	18 (17.14%)	75	71.43	U
8	Advance fee fraud	10 (9.52%)	7 (6.67%)	15 (14.29%)	9 (8.57%)	7 (6.67%)	13 (12.38%)	61	58.10	U

Key: N.W= North West Zone: N.E=North East Zone: N.C= North Central Zone: S.S= South South Zone: S.W= South West Zone: S.E= South East Zone: D=Decision; U=Upheld; NU=Not Upheld

Table 1 showed that all the listed cybercrimes existed in Nigerian Federal University Digital Libraries. The list of cybercrimes conforms to that which Lu, Jen and Chou (2006) considered most common across national and cultural boundaries. Rathinasabapathy and Rajendran (2007) also observe that these cybercrimes exist in academic libraries in India.

Findings from Federal University digital libraries in the geo-political zones

showed that in North West, scam mails, Internet pornography and data theft ranked first. In North East, Internet pornography and data theft ranked first while in North Central scam mails ranked first. In South South, Internet pornography and data theft ranked first. In South West, scam mails ranked first while in South East, Internet pornography ranked first.

Table 2: Percentage Response on Stakeholders Involved in Controlling Cybercrime in Federal University Digital Libraries N=105

Geopolitical Zones in Nigeria										
Stakeholders	N.W	N.E	N.C	S.S	S.W	S.E	Total	%	D	
1 Staff in charge of computer systems	13 (12.38%)	10 (9.52%)	28 (26.67%)	17 (16.19%)	14 (13.33%)	16 (15.24%)	98		U	
2 University security personnel	7 (6.67%)	6 (5.71%)	18 (17.14%)	9 (8.57%)	6 (5.71%)	12 (11.43%)	58	55.23	U	
3 Library Administration	13 (12.38%)	10 (9.52%)	25 (23.81%)	16 (15.24%)	11 (10.48%)	13 (12.38%)	88	83.81	U	
4 All library workers	9 (8.57%)	4 (3.81%)	12 (11.43%)	6 (5.71%)	8 (7.62%)	8 (7.62%)	47	44.76	N U	
5 All users of the cybercafé	7 (6.67%)	5 (4.76%)	10 (9.52%)	6 (5.71%)	7 (6.67%)	7 (6.67%)	42	40.00	N U	

Key: N.W.=North West Zone: N.E.= North East Zone; N.C= North Central Zone; S.S= South South Zone; S.W= South West Zone; S.E= South East Zone; U=Upheld; NU=Not Upheld; D=Decision

Table 2 shows that stakeholders who control cybercrime in University digital libraries are staffs in charge of computer systems, security personnel posted to

the library and library administration. The finding indicates that there are specific people saddled with the responsibility of controlling cyber-

crimes. This finding contradicts the assertion of Akuta, Ong'oa and Jones (2011), which states that stakeholders in the fight against cybercrime in sub Saharan Africa range from the average man on the street to the president of the particular nation. The respondents'

rejection of the option of "all library workers and all cybercafé users" as stakeholders in fighting cybercrime is a further pointer to the fact that the suggestion of Akuta, Ong'oa and Jones (2011) is not based on popular opinion.

Table 3: Mean Response on Strategies Used in Controlling Cybercrimes in Federal University Cybercafés in Nigeria N=105.

Strategies	Geopolitical Zones in Nigeria							Decision
	X _{N.W.}	X _{N.E.}	X _{N.C.}	X _{S.S.}	X _{S.W.}	X _{S.W.}	X _{g.}	
1 Use of bill boards	3.31	3.20	3.68	3.29	3.0	3.24	3.29	Upheld
2 Use of Notice boards	3.54	3.20	3.72	3.12	2.83	3.29	3.28	Upheld
3 Use of electronic gadgets	3.62	3.40	3.66	2.65	2.93	3.38	3.27	Upheld
4 Stationing of Security men in Libraries	3.31	2.70	3.03	2.94	2.93	3.33	3.04	Upheld
5 Use of Content Filter Soft wares	3.54	3.00	3.28	2.82	3.21	3.33	3.20	Upheld

Key: X_{N.W.} = Mean for North West Zone; X_{N.E.} = Mean for North East Zone; X_{N.C.} = Mean for North Central Zone; X_{S.S.} = Mean for South South Zone; X_{S.W.} = Mean for South West Zone; X_{S.E.} = Mean for South East Zone and X_{g.} = Mean of Means/Grand Mean

Table 3 showed that respondents accepted all the items as strategies used for controlling cybercrimes. Use of bill boards topped the list. It had a grand mean of 3.29. It confirms the assertion made in the literature by Longe & Chiemeké (2008) that it is a common thing on Nigerian roads to see bill boards warning cybercriminals of their

impending doom. Use of notice boards had a grand mean of 3.28 and was the second highest accepted strategy. Simple observation at University of Nigeria, Nsukka cybercafés reveals that the walls of the cybercafés are donned with notices warning cybercriminals to desist from the act or face the wrought of the Law.

Table 4. Mean Response on Challenges of Controlling Cybercrime in Nigerian University Cybercafés N = 105.

Challenges	Geopolitical Zones in Nigeria							Decision
	X _{N.W.}	X _{N.E.}	X _{N.C.}	X _{S.S.}	X _{S.W.}	X _{S.W.}	X _{g.}	
1 Library laws and regulations do not cover cybercrimes	3.31	3.00	3.34	3.24	3.20	3.29	3.23	Upheld

2	The workers are not skillful in detecting offenders	3.38	3.20	3.31	3.24	2.87	2.81	3.14	Upheld
3	The offenders are too numerous to be managed	2.77	2.80	2.72	2.76	2.60	2.71	2.73	Upheld
4	There is no fund to procure cybercrime detecting equipment	2.54	3.00	3.41	3.12	3.07	3.29	3.07	Upheld
5	Staffs connive with the offenders to conceal the crime	2.54	2.80	2.44	2.18	2.33	2.14	2.41	Not Upheld

Table 4 showed that respondents accepted non-coverage of cybercrime by library laws and regulations as the greatest challenge in combating cybercrime. The finding is in line with the observation of Akuta, Ong'oa and Jones (2011) which states that existing laws in Nigeria do not cover cybercrime. The laws regarded computers as properties and could only prosecute criminals that were involved in stealing the whole computer system or destruction of the computer but had no jurisdictional powers over information hackers. . Respondents also agreed that offenders were becoming numerous and intractable. The finding confirms the observation of Lu, Jen and Chou (2006) which state that the number of cybercrime perpetrators among college and graduate students is increasing in geometric progression. Staff connivance with cybercrime offenders was rejected by respondents. This response gives credence to the general belief that librarianship attracts mostly people of humble and caring disposition

Discussion of Findings

Finding from the study shows that types of cybercrimes exist in Federal University Libraries in Nigeria. The highest cybercrime committed in these institutions was internet pornography. This is consistent with the findings of Laumbano and Nawe (2004) in which it was discovered that majority of the students of Dar es Salaam University used internet to view pornography. Lu, Jen and Chou (2006) listed cyber pornography and spreading messages related to sex trading on the internet among five top cybercrime offences that take place in Taiwan every year. Scam mails were the second highest cybercrime. The Internet Crime Report (2008) of National White Collar Crime Centre observed that Nigerian letter fraud constituted 5.2% of the reported total economic loss through cybercrime for the year 2008. Data theft was the third highest cybercrime. Ewuuk and Shannon (2009) note that data theft and malicious break-ins are prevalent.

The study identified stakeholders who controlled cybercrime in University digital libraries. This implies that there are specific people saddled with the

responsibility of controlling cybercrimes. For any action to make a meaningful impact, the responsibility for that action must be vested on a specific individual or group of people. Finding also showed that university security personnel should control crime in the libraries. The finding agrees with Curry, Flodin and Matheson (2000) who opine that mere presence of security personnel within the library acts as an effective deterrent to would-be thieves and vandals.

Use of bill boards was found to be the greatest strategy used in controlling cybercrimes. It confirms the assertion made in the literature by Longe & Chiemeka (2008) that it is a common thing on Nigerian roads to see bill boards warning cybercriminals of their impending doom. Akuta, Ong'oa and Jones (2011) opined that EFCC, the body saddled with the responsibility of controlling cybercrime in Nigeria, should use software called Eagle Claw in its operations. The researchers concurred that the software would facilitate sniffing out of fraudulent emails.

The study also found that library laws and regulations did not cover cybercrime. The omissions constitute critical challenge to the control of cybercrimes. The finding is in line with the observation of Akuta, Ong'oa and Jones (2011) which states that existing laws in Nigeria do not cover cybercrime. Boateng, Olumide, Isabalija and Budu (2011) observe also that the laws of many nations do not cover cybercrime. Wada and Odulaja (2012), posit that presently, there is no law specific to

cybercrime in Nigeria. Lack of skill of cybercafé workers in detecting cybercriminals constitutes a challenge in controlling cybercrimes. Lack of skill of cyber workers also offers cybercriminals the required opportunity to carry out the heinous act without disturbance. The opportunity theory as stated by Wada and Odulaja (2012) posit that no crime can occur without the physical opportunity and therefore opportunity plays a role in cybercrimes. Lack of funds to procure cybercrime detecting machine was also a challenge. This is expected considering the ongoing global economic recession.

Recommendations

From the findings and conclusion, it is recommended that in order to control upsurge in cybercrimes, Federal University Libraries should:

1. Include and entrench stiff penalties against cybercrime in University laws and regulations.
2. University administration should post security staff routinely to University Library cybercafés to instill discipline.
3. Library administration should as a matter of urgency, procure and install Content filters software and cybercrime detecting equipment in all library and university cybercafés.
4. Bill boards and notice boards should be used as awareness tools to warn people of cybercrimes.
5. Library Administration should guard against anybody feigning ignorance of the law.
6. Closed circuit television and other electronic gadgets should be installed and used to monitor users.

Conclusion

From the findings of the study it is concluded that the greatest cybercrimes committed in Nigerian Federal University digital libraries are internet pornography and scam mails. It can be concluded that in the ranking order, the greatest stakeholders in the control of cybercrimes are the staffs in charge of the computer systems, the library administration and university security personnel who are posted to guard the university cybercafés. It is also concluded in this study that non-coverage of cybercrimes under library laws and regulations constitute critical challenge to the control of cyber-crimes.

References

- Akuta, E. Ong'oa, I & Jones C. (2011). Combating cybercrime in Sub-Saharan Africa: A discussion on law, policy and practice. *Journal of Peace, Gender and Development Studies* 1 (4), 129-137.
- Asokhia, M. (2010). Enhancing National Development and Growth through combating cybercrime/Internet fraud: A comparative approach. *Journal of Social Science* 23 (1), 13-19
- Association of Commonwealth Universities, (2008). *Commonwealth Universities Yearbook 2008*. vol. 1, 82nd. edition, UK CPI William Clowes Beccles. 1127 - 1217
- Boateng, B., Longe, O. , Mbarika, V. , Awevor, I. & Isabalija, S. (2010). Cybercrime and criminality in Ghana: Its forms and implications. *Proceedings of the 16th Americas Conference on Information Systems*, Lima, Peru August 12-15.
- Boateng, Olumide, Isabalija & Budu, S. (2011). Cybercrime and criminality in Ghana. *Journal of Information Technology Impact*. 11 (2), 85 - 100.
- Curry, A., Flodin, S. & Matheson, K. (2000). Theft and mutilation of library materials: Coping with Biblio-Bandits. *Library and Archival Security*. 15 (2), 9-26
- Ehimen, B. & Bola, A (2010). Cybercrimes in Nigeria. *Business Intelligence Journal*. 3 (1), 94-98.
- Ewuuk, D . & Shannon, L. (2009). Perceptive profiles of students' computer security and safety competencies: Implications for business curriculum. *Issues in Information Systems*. X:2, 299-308
- Laumbano, I. & Nawe, J. (2004). Internet use among the students of University of Dar es Salaam. *Library High Tech News*. 21 (10), 13-17
- Longe, O & Chiemeké, S. (2008) Cybercrime and criminality in Nigeria - What roles are Internet Access points Playing. *European Journal of Social Sciences* 6 (4), 132-139.
- Lu, C. Jen, W, Chang, W. & Chou, S. (2006) Cybercrime & Cybercriminals: An Overview of the Taiwan Experience. *Journal of Computers*. 1 (6), 1-8.
- Lu, C., Jen, W., Chang, W. & Chou, S. (2008) Cybercrime and Criminality: An overview of the Taiwan Experience. *Journal of Computers*, 1 (8), 11-17.
- National White Collar Crime Centre, (2008). *Internet Crime Report 2008*. Available at : [http:// www.nw3c.org](http://www.nw3c.org). accessed on Sept. 12, 2012.
- Padhye, V. & Gujar, M. (2012). Virtual impersonation by anti-social personalities in cybercrime. *DAV International Journal of Science*. 1 (2), 49-52
- Rathinasabapathy G. & Rajendran, L. (2007). Cybercrimes and information frauds: Emerging challenges for LIS professionals. *Proceedings of the Conference on recent advances in Information Technology READIT - 2007 organized by Madras Library Association Kalpakkam Chamber & Scientific Resources Division, Indira Gandhi Centre for Atomic Research Kalpakkam 603 102, Tamil Nadu*. July 12 & 13, 2007. Available at: <http://www.igcar.ernet.in/igcar2004/sird/r>

edit2007.pdf#page=159pages131to168.

Accessed on November 11 2012

Wada, F. & Odulaja, G.O (2012). Assessing cybercrime and its impact on E-Banking in

Nigeria, using social theories. *African Journal of Computing & ICT*.4 (3) , 69 -82.

Appendix 1. Universities that participated in the study

Geopolitical Zones		Number and names of Federal Universities	No of Librarians in each Cybercafé.	
			Respondents	Population
North Central	1	Federal University of Technology, Minna	5	5
	2	University of Agriculture, Makurdi	5	5
	3	University of Abuja	7	7
	4	University of Jos, Jos	5	5
	5	University of Ilorin, Ilorin	7	7
North East	6	Abubakar Tafawa Balewa University (ATBU).	3	3
	7	Federal University of Technology, Yola	3	3
	8	University of Maiduguri	4	4
North West	9	Ahmadu Bello University (ABU)	5	8
	10	Bayero University Kano	4	4
	11	Usman DanFodiyo University, Sokoto	4	4
South East	12	Federal University of Technology, Owerri	8	8
	13	Nnamdi Azikiwe University, Awka	2	2
	14	University of Agriculture, Umudike - Umuahia	4	4
	15	University of Nigeria, Nsukka	7	10
South West	16	Federal University of Agriculture, Abeokuta	3	3
	17	Obafemi Awolowo University, Ile- Ife.	2	5
	18	Federal University of Technology, Akure	2	2
	19	University of Ibadan	5	8
South South	20	University of Lagos, Lagos	3	6
	21	University of Benin	4	4
	22	University of Calabar	4	4
	23	University of Port Harcourt	4	4
	24	University of Uyo	5	5
SIX GEO-POLITICAL ZONES	Total	24 FEDERAL UNIVERSITIES	105	120