MANAGEMENT OF CYBER SECURITY CHALLENGES IN TERTIARY INSTITUTIONS IN SOUTH-EAST NIGERIA

Obioma, Emmanuel Anyakamunelechi
Department of Educational Foundations
Faculty of Education, University of Nigeria, Nsukka

Abstract

Cyber space is the boundless area called the internet. The internet is also being faced by security challenges. Cyber security refers to the body of rules and regulations put in place for the protection of cyber space. On the other hand, cyber-crime involves the series of organized crime attacking the internet as well as cyber security. The internet therefore remains one of the fastest growing areas of technology development with many infrastructures. Recently, the growths of the internet and its uses have provided everyone this opportunity. Wikipedia, Goggle and Bing among others provide detailed answers to millions of questions on daily basis to people that require them. Internet is a world that contains anything one is searching for. Thus, with the coming of these technologies in information accessibility and their merits in their applications come with increasing demerits. This has increased cyber security which has become a national concern due to its threats not only to individuals, but also organizations including educational institutions. This has to be checked and tackled seriously in the present day society. This paper explored cyber-crime, internet security management, the nature, reasons, and areas of involvement by people as they relate to security in the administration and educational institutions in South-East, Nigeria.

Key words: Cyber space, cyber-crime, cyber security, ICT, institutions, management

Introduction

The advent of internet is a welcome development globally that has both advantages and disadvantages. It comes along with crimes as well as its associated security challenges. The incidence of cyber-crime in Nigeria in recent times has been quite alarming with its negative impact on the socio-economic and educational enterprises. Cyberspace users over the years have continued to use the internet to promote crimes which have had and continued to have untold consequences on the people. There has been unprecedented and extra ordinary increase in cybercrime and security challenges not only in Nigeria, but also in other parts of the world. For instance, the first ever recorded cyber crime incidence was committed in the United States of America while in Nigeria cyber crime is being witnessed as an innovative phenomenon by people.

Cyber crime in Nigeria is taking different dimensions. Recently the country has acquired a world-wide notoriety in criminal activities especially involving scams accelerated through the use of the internet (Rose & Moses 2012). Cyber-crime refers to crimes that take place in the internet (Almed, Al-khater, Al-Maadeed, Sadiq, & Khan, 2020). The high incidence of cyber-crime has led to the advent of cyber security, which aims to tackle the problems or reduce cyber-crime related or associated issues. Cyber-crime involves criminal activities done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrimes also include non-monetary offenses, such as: creating and distributing viruses on other computers or posting confidential business information on the internet. Perhaps, the most prominent form of cybercrime is theft, in which criminals use the internet to steal personal information from other users. Recently, most businesses including educational institutions appear to adopt digital cloud indicating that the services rendered in cloud transaction are fully saved and secured. However, information technology professionals are beginning to fear the security of such cloud transactions, because of its associated risks of data storage. People are afraid of individuals and organizations revealing vital information through cloud security. Hence, there is the need to come up with intervention measures to safeguard cloud information and data from fraudulent users (Laura, 2014). However, cloud security appears to be one of the major security measures towards tackling the problems of cyber crime in the society.

Cloud security is meant to protect customers' data, orders, blueprints and other information. Breach of data and theft must be avoided at all cost to preserve customer trust and secure the access that allows one to gain a competitive advantage. The essence of cloud based security is to secure data and resources crucial for any firm or institution moving to the cloud. Any educational institution that wants to keep its data safe from crooks must invest as much as possible in cloud computing security. Such institution may gain the advantages of cloud computing, which are now widely acknowledged by maintaining a robust cloud stance. Cloud security comes with its own sets of advantages, such as reduced upfront cost, lower ongoing administrative cost, easier stability, stronger stability and availability as well as better distributed denial of service protection (Ponemon Institute, 2019). Cloud security is a cyber-security that focuses on ensuring the security of cloud computing systems. It involves safeguarding private data and security across the internet infrastructure, applications and platforms (Badejo, Okuneye & Taiwo, 2018). Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practice, assurance and technologies that can be used to protect the cyber environment, institutions and user's assets. Organization and user's assets including: connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and /or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Cyber-security is the body of rules put in place for the protection of cyber space. It becomes expedient to critically examine the goals of cyber security.

The goals of cyber security among others include to: help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks; help individuals and institutions develop and nurture a culture of cyber security; work collaboratively with public, private and international entities to secure cyberspace. The goals also help to understand the current trends in IT/cybercrime, and develop effective solutions which may include authenticity, non-repudiation and confidentiality, all aimed at providing adequate security for users' information. Cyber service providers and their customers' efforts are aimed at ensuring how an organization or institution goes about protecting these systems. To host services on their servants, cloud providers employ an all-time internet connection since their business depends on customer's trust that utilizes cloud security to keep client information private and safe. Hence, it has become imperative to find out or determine the type of management practices by different educational institutions to safeguard their websites and manage their data effectively (Lukfaldt & Holt, 2022).

Educational institutions are institutions who are involved in data management in different aspects of research and learning. These information need to be well protected from other individual users who are also interested in cyber security management of their data. Most educational institutions are now digital-based and operate cloud computing system with their information or data being managed online. Since cyber-crime is committed in the internet, it becomes imperative that institutions employ adequate cyber security management system to protect their data being tampered with by unknown persons or hackers. This is because many institutions use computer networks to perform complex activities. The electronic economy is open to everyone including criminals. The bulk of successful intrusions according to various studies targets exploitable vulnerabilities in the application layers, underscoring the necessity for ICT company personnel to be extremely diligent on application security (Eluwah, 2021). Application security is one of the cyber security management procedures employed by institutions targeted at protecting their entire life span against any threat. To sensitive data and confidential materials, cyber-criminal is organized, competent and motivated to locate and exploit loopholes in intuitional system. Application of security management is used to assist organizations or institutions in all types of applications such as desktop, website, mobile, and micro services used by public and private stakeholders such as customers and workers required of application security solutions. Application security solutions must be able to test web application for possible and exploitable possibilities, analyze code and assist the security and defense management processes by promoting collaboration and facilitating communication among diverse users (Muhattan, 2015).

There are other methods educational institutions can apply cyber security management practices to safeguard their data from the hands cyber criminals. Cyber security practices constitute actions taken by educational institutions to ensure cyberspace safety from known and unknown threats. World-wide, cyber security practices have been experienced and are still being experienced by public and private organizations and institutions. Among such practices include: login authentication, access control, scanning data/information malware, antivirus installation and regular update, use of firewall protection and login out or shutdown institutional computers among others. These cyber security management practices by institutions are applied to checkmate the activities of cyber criminals on institutions' data (Chikwuendu & Oli, 2023).The use of password management by institutional managers is to help in preventing and identifying employee leakage of information from institutional data base. However, because data mining software cannot rapidly handle massive volumes of data and does not allow programmers to precisely focus suspicion on a specified type of crime, this strategy can only work in institutions with small data base. These practices appear to be very much commonly applied by institutional staff (Shackelford, 2012). Also, research studies have shown that access control and use of firewall protection, antivirus installation and regular update as well as login and shutdown institutional system or computers remain high as applied cyber security practices by institutions to control the activities of unknown persons or threats in their data management (Trend, 2020).

The above measures or practices notwithstanding, cyber criminals are known to disseminate spyware by gaining a person's trusts and inducing such individual to visit a website. Institutions must encourage their employees or staff to be careful about any link, file application and web page they come across online. This is because most cyber security architectures may be the generic passwords mostly used by hackers. Hackers can readily guess login credentials and take over using brute force attack tactics (Kelvin, 2022). The only way to eliminate this risk is for the institution's employees to use strong unique passwords and complicated passwords. As technology has developed, so have the definitions of cyberspace, cyber security and cybercrimes. It has been argued that since computer crime may involve all categories of crime, a definition must emphasize the particularity, the knowledge or use of computer technology. Ensuring cyber-security requires coordinated efforts from both the citizens of the country and the country's information system. Previous studies have shown that cyber challenges may include: Illegal Access (Unauthorized Access) to institutional Computers and Illegal interception of institutional data or information among other (Olumide & Victor, 2010; Moses-Oke, 2012).

Statement of the problem

The threat posed by breaches in institutions' cyber-security is advancing faster than can be imagined. It is not possible to concentrate on only one aspect of the breach as it means negligence and allowance of growth for other aspects of the breach. In most tertiary institutions in South-East, there appears to be poor cyber security arrangements for effective security management. This situation poses a serious challenge to school principals as their database seems to be exposed to cyber security test. Against this background, this paper investigated the management of cyber security challenges in tertiary institutions in South-East, Nigeria.

Purpose of the Study

The aim of this study is to investigate the management of cyber security challenges in tertiary institutions in South-East, Nigeria**.** Specifically, the study determined:

1. Cyber security challenges faced by tertiary institutions in South East Nigeria and
2. Cyber security management practices available in such institutions.

Research Questions

The following research questions guided the study.

1. What are the cyber security challenges in tertiary institutions in South East, Nigeria?
2. What are the cyber security management practices in tertiary institutions in South East, Nigeria?

Hypotheses

The following null hypotheses were formulated to guide the study and were tested at 0.05 level of significance.

Ho$_1$: There is no significance difference between administrative officers and ICT personnel on the cyber security challenges facing tertiary institutions in South East, Nigeria.

Ho$_2$: There is no significance difference between administrative officers and ICT personnel on the cyber security management practices in tertiary institutions in South East, Nigeria.

Methods

The study adopted a descriptive survey design. The population comprised 820 respondents made up of 480 administrative officers and 340 ICT personnel in University of Nigeria, Nsukka and Abia State University, Uturu. The population made up the sample size since the sample size is manageable. The instrument for data collection was a researcher-designed questionnaire titled 'Cyber Security Challenges and Management Practices Questionnaire (CSCMPQ)'.The questionnaire was arranged into two clusters – A & B structured on 4-point rating scale of Strongly Agree (SA), Agree (A), Disagree (D) and Strongly Disagree (SD). The instrument was validated by three experts from the Department of Educational Foundations and Science Education Department all in the Faculty of Education, University of Nigeria, Nsukka. The overall reliability estimate of the questionnaire was 0.88 obtained using Cronbach Alpha method. Mean and standard deviation were used in answering the research questions while t-test was used in testing the hypotheses at 0.05 level of significance.

Results

Research Question One: What are the cyber security challenges in tertiary institutions in South East, Nigeria?

Table 1: Mean responses and standard deviation of the administrative and ICT staff on the cyber security challenges in tertiary institutions in South East Nigeria

S/N	Item statements	Mean	SD	Dec
1.	Illegal Access (Unauthorized Access) To Institutional Computers	3.21	0.72	Agree
2.	Illegal interception of institutional data or information	3.39	0.65	Agree
3.	Interfering with the functioning of institutional computer system	3.12	0.90	Agree
4.	Suppressing computer data	3.20	0.93	Agree
5.	Misuse of office devices	2.84	0.86	Agree
6.	Internet theft	3.08	0.89	Agree
7.	Antivirus problems	3.28	0.84	Agree
8.	Incompetence ICT personnel	3.17	0.73	Agree
	Grand mean	**3.21**	**0.98**	**Agree**

Table 1 shows the responses of administrative and ICT staff on the cyber security challenges facing tertiary institutions in South-East, Nigeria. The table reveals that all the items 1-8 are security challenges and had their mean scores above the criterion mean of 2.50. This implies that, the respondents are in agreement that all the listed items are cyber security challenges facing tertiary institutions in South-East Nigeria. The above was supported with their grand mean score which is 3.21.This implies that tertiary institutions in South-East Nigeria are faced with cyber security challenges in their management as identified above.

Hypothesis One: There is no significance difference between the mean scores of administrative officers and ICT personnel on the cyber security challenges facing tertiary institutions in South East, Nigeria**.**

Table 2: t-test analysis of the responses of administrative officers and ICT personnel on the cyber security challenges in tertiary institutions in South East Nigeria

S/N	Group	N	Mean	SD	df	t-cal	Level of sign	Dec

1	Administrative officers	480	3.09	0.72	818	0.00	0.05	Accept (NS)
2	ICT personnel	340	3.22	0.66				

Table 2 shows that the calculated t-value of 0.00 is less than 0.05 level at 818 degree of freedom. Therefore the null hypothesis is accepted. This implies that, both administrative officers and ICT personnel did not differ in their opinions on the challenges of cyber security in tertiary institutions in South-East Nigeria. Therefore, there is no significant difference between the mean scores of administrative officers and ICT personnel on the challenges of cyber security in tertiary institutions in South East, Nigeria.

Research Questions Two: What are the cyber security management practices in tertiary institutions in South East, Nigeria?

Table 3: Mean responses and standard deviation of the administrative and ICT staff on the cyber security management practices in tertiary institutions in South East, Nigeria

S/N	Item statements	Mean	SD	Dec
9.	Use of protective passwords	3.40	0.82	Agree
10.	Antivirus installation	3.11	0.86	Agree
11.	Password protection	3.33	0.71	Agree
12.	Data encryption	3.07	0.76	Agree
13.	Compulsory logout from system when not used	3.35	0.69	Agree
14.	Use of official e-mails only for official correspondents	3.03	0.88	Agree
15.	Regular upgrades of antivirus	2.80	0.97	Agree
16.	Employment of ICT expert	2.98	0.86	Agree
Grand mean		**3.05**	**0.82**	**Agree**

The data on table 3 show the mean responses and standard deviation of the administrative and ICT staff on the cyber security management practices applied in tertiary institutions in South East, Nigeria. The result shows that all the items 9-16 had their mean scores ranging from 2.80-3.40, which are above the criterion mean of 2.50 for acceptance of an item as an agreement. This is an indication that the administrative and ICT staff are in agreement that the items are cyber security management practices applied in tertiary institutions in South-East Nigeria. The above implies that administrative and ICT staff is in agreement that tertiary institutions in south east apply cyber security management practices.

Hypothesis Two: There is no significance difference between the mean scores of administrative officers and ICT personnel on the cyber security management practices in tertiary institutions in South East, Nigeria.

Table 4: t-test analysis of the responses of administrative officers and ICT personnel on the cyber security management practices in tertiary institutions in South

S/N	Group	N	Mean	SD	df	t-cal value	t-critical value	Level of sign	Dec
1	Administrative officers	480	3.11	0.83	818	0.613	1.89	0.05	Accept (NS)
2	ICT personnel	340	3.20	0.78					

East Nigeria

Table 4 shows that, the calculated t-value of .000 is less than 0.05 level at 818 degree of freedom. This means that the null hypothesis is accepted. This implies that both administrative officers and ICT personnel did not differ in their opinions on the cyber security management practices applied in tertiary institutions in South-East Nigeria. Therefore, there is no significant difference between the mean scores of administrative officers and ICT personnel on the cyber security management practices in tertiary institutions in South East Nigeria.

Discussion

This study identified cyber security challenges to include: illegal access (unauthorized access) to institutional computers, illegal interception of institutional data or information, interfering with the functioning of institutional computer system, suppressing computer data and misuse of office devices among others. The findings of the study above are in line with the results of Olumide and Victor, (2010); Moses-Oke (2012) who in their views pointed out that cyber security challenges are illegal access (unauthorized access) to institutional computers and illegal interception of institutional data or information. The result of the hypothesis revealed that administrative officer and ICT personnel did not differ significantly on the cyber security challenges in tertiary institutions in South-East Nigeria.

The findings of the study identified the following as cyber security management practices applied in tertiary institutions in South East Nigeria - use of protective passwords, antivirus installation, password protection and data encryption. Other management practices include compulsory logout from system when not used, use of official e-mails only for official correspondents, regular upgrades of antivirus and employment of ICT expert. The above findings are in consonance with the findings of Chikwendu and Oli (2023) who in their study identified regular upgrades of antivirus, employment of ICT expert, and use of passwords among others as cyber security management practices in tertiary institutions in South-East Nigeria. The findings are also in line with the opinion of Shackelford (2012) who also asserted that compulsory logout from system when not used as management practices in tertiary institutions in South-East Nigeria. Also, the second hypothesis of no significant different of the study was accepted implying that administrative officers and ICT personnel did not differ significantly on the application of cyber security practices in tertiary institutions in South-East Nigeria

Educational Implications of the Findings

The result of the study has implications for the institutions and their workers. The institutions are to be cyber security conscious to ensure proper institutional data protection and also ensure that their information systems are protected by unauthorized access to maintain their academic credibility. Also to ensure continuity of academic activities, they have to be mindful of ineffective cyber security management which may cause cyber attacks. Apart from the above, the institutions in South-East are to prevent cyber attacks that may lead to financial loses.

Conclusion

It was concluded that the institutions in South East Nigeria apply cyber security management practices in their operations with some challenges. Therefore, there is need for the institutions to look inwards to ensure effective and efficient cyber security arrangement

Recommendations

Based on the conclusions, the following recommendations were made.

1. Institutions should be made to guide actively their data base to avoid interference by unknown persons or cyber criminals. More sensitization should be carried out through seminars and workshop to educate the staff of the institutions on the various ways to checkmate the activities of cyber criminals
2. The institutions should embrace the identified cyber security management practices to ensure proper security of their data in the internet.

REFERENCES

Bauer, J. M. & VanEeten, M. J. (2009). The Economics of Spam. In S. Dietrich (Ed.), *Economics of Information Security* 259-308.

Chikwendu, S. C. & Oli, N.P(2023).Cyber Security Practices in Public Universities in South-East Nigeria. *Practicum Psychologia http://journals.aphriapub.com/index*.php.pp13,

Eluwah, D. (2021). Cyber Awareness and Education in Nigeria: An Assessment. 10.13140/RG.2.2.23425.79202.

Kelvin, J. (2022). Importance of Cybersecurity in the education sector https://cybersecurityforme.com/imporrtance-of-cybersecurity-in-education/

Laura, A. (1995). Cyber Crime and National Security: The Role of the Penal and Procedural Law" , Nigerian Institute of Advanced Legal Studies., Retrieved from http://nials-nigeria.org/pub/lauraani.pdf Longe, O. B, Chiemeke, S. (2008): Cyber Crime and Criminality In Nigeria – What Roles Are Internet Access

Olumide, O. O.& Victor, F. B. (2010). E-Crime in Nigeria: Trends, Tricks, and Treatment. The *Pacific Journal of Science and Technology*, 11, 1.o

Ponemon Institute. (2019). The Cost of Cyber Crime Study: Global. Retrieved from https://www.ponemon.org/local/upload/file/2019%20Global%20CC%20Study%20FI
NAL%209-4.pdf

Moses-Òkè R. O. (2012). Cyber Capacity Without Cyber Security: A Case Study of Nigeria's National Policy For Information Technology (NPFIT), *The Journal of Philosophy, Science & Law*, Retrieved from www.Miami.Edu/Ethics/Jpsl

Shackelford, S. J. (2012). *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge University Press.

Trend Micro Inc. (2020). *Annual Cybersecurity Report*. Retrieved from19-39 https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threatreports/annual-