IJAAR PUBLISHING®

International Journal of Education and National Development | ISSN: 3027-0626
Vol. 2, Issue 1 (January-March, 2024) | www.ijaar.org

Digitalizing cyber security for data management in higher education: Implication for Educational Management in Nigeria.

By

Emmanuel Sunday Essien

&

Egbeji Emmanuel Edun

Department of Educational Management, Faculty of Education, Cross River University of Technology, Calabar.

E-mail: emmanuelessien25@yahoo.com

Abstract

This study was to determine digitalizing cyber security for data management in higher education: Implication for Educational Management in Nigeria. Two research questions and hypotheses were formulated to guide the study. The population of this study comprises 4000 students from four tertiary institutions in Cross River State. The sampling technique employed by the researcher in the selection of the sample was the simple random sampling technique. The sample size selected for this study was 400 students in selected schools which represents 10 percent of the accessible population comprising of 200 males and 200 females. The questionnaire was designed to measure the two sub-independent variables. The reliability of the instrument was 0.85 reliability coefficient. Mean and standard deviation were used to answer the research questions. While Simple linear regression analysis statistical tool was used to test the null hypotheses that were formulated to guide the study at 0.05 level of significance. The findings of the study show that the educators' lack of knowledge and expertise regarding cyberspace in tertiary institutions significantly influence cyber security knowledge in data management in tertiary institutions and Cyber security knowledge in data management in tertiary institutions significantly reduces cyber-bully, online fraud, racial abuse, pornography and gambling among educators and students in tertiary institutions in Cross River State, Nigeria. Based on the conclusion, it was recommended that tertiary institutions management should formulate educational policies and curriculum the will help in addressing problems of cybercrime in schools. And students and educators should learn Cyberspace knowledge since it is very important in their day to day activities.

Keywords: *Educators, Cyberspace, Tertiary institutions, Cyber security, Data management.*

Essien, S. E. & Edun, E. E. (2024). Digitalizing cyber security for data management in higher education. Implication for Educational Management in Nigeria. *International Journal of Education and National Development*. 2(1), 70-78.

Introduction

The main purpose of education especially at the tertiary level is to empower an individual to excel in a chosen field of endeavor or career, and to be able to positively impact on his/her society and as such educational systems play an important role in the development of an individual which increases in line with the number of trained and equipped individuals. For this reason, innovative educational practices have become obligatory because they form the foundations that enhance the growth of students.

The advancement in technology is gradually affecting students and educational environment as most educators lack knowledge and expertise regarding cyberspace and cyber security for data managementin schools. Data are raw facts, events, numbers and transactions, which have been collected, recorded, stored but are not yet processed. Data, according to Alzighaibi (2021) consist of numbers, characters, alphabets and special symbols which are used to record facts and events about activities occurring in an environment. Information is processed data. It is obtained after subjecting data to a series of processing operations which convert related groups of data (raw facts) into a meaningful and coherent form. Processing could be in the form of addition, subtracting, comparison, sorting, rearrangement etc. This makes information useful and meaningful. In other words, information could be defined as the desired form to which data is finally transformed after undergoing a series of processing. This data may be students name, Matriculation number, students' scores, staff records and school records.

Data management includes all aspects of data planning, handling, analysis, documentation and storage, and takes place during all stages of a study. The objective is to create a reliable data base containing high quality data. Data management is a too often neglected part of study design,1 and includes: Planning the data needs of the study, data collection, data entry, data validation and checking, data manipulation, data files backup and data documentation in higher education (Alzighaibi, 2021).

Higher institutions and government ministries in Nigeria are also lacking resources and facilities to implement cyber security education. According to Rahman, Sairi, Zizi, and Khalid (2020), Cyber security is the activity, process, ability or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorised use or modification, or exploitation challenges schools face in implementing.

The speed of technological change results in new risks, requiring new solutions. Educators are face with the problems in developing their knowledge of the latest technology and thus ensuring students are safe, there is need to digitalized cyber security for data management in higher education asCyber Crime is on the increase and Cyber security education is inevitable since information and communication technology which enabled learning possesses are threatened (Anekw, 2017).

RESEARCH QUESTIONS

This study is guided by the following research questions:

1. To what extent does the educators' lack of knowledge and expertise regarding cyberspace in tertiary institutions significantly influence cyber security knowledge in data managementin tertiary institution?

2. To what extent does cyber security knowledge in data management in tertiary institutions significantly reduce cyber-bully, online fraud, racial abuse, pornography and gambling among educators and students in tertiary institution in Cross River State, Nigeria?

STATEMENT OF HYPOTHESES

Two hypotheses were postulated and tested at .05 level of significance. They are;

Ho1: The educators' lack of knowledge and expertise regarding cyberspace in tertiary institutions does not significantly influence cyber security knowledge in data management in tertiary institutions.

Ho2: Cyber security knowledge in data management in tertiary institutions does not significantly reduce cyber-bully, online fraud, racial abuse, pornography and gambling among educators and students in tertiary institution in Cross River State, Nigeria.

METHODOLOGY

Research design: The study adopted the descriptive research design. The research covered all public and private tertiary institutions. The population of this study comprises 4000 Educators and students from four higher institutions in Cross River State. The sampling technique employed by the researcher in the selection of the sample was the simple random sampling technique. The questionnaire were designed to measure the three sub-independent variables. Mean and standard deviation were used to answer the research questions. While Simple linear regression analysis statistical tool was employed to test the null hypotheses that were formulated to guide the study at 0.05 level of significance.

Instrumentation: A structured questionnaire designed by the researcher was used to collect the needed data in this study. This is titled "Digitalizing Cyber Security for Data Management in Higher Education for Educational Management (DCSDMHEMQ) questionnaire. The reliability of the instrument was determined, using the Cronbach Alpha method which involved 30 year one students who were not part of the sample used in the study. The reliability of the instrument was 0.85 reliability coefficient.

Sample and Sampling Procedure: The stratified random sampling technique was used to select 400 staff and students in selected schools which represents 10 percent of the accessible population comprising of 4000 males and females staff and students which gives the total sample size used for the study. Contacts were made with the selected tertiary institutions where respondents were briefed on the aim and importance of the study and their cooperation solicited with regards to their responses to the questionnaire items. After two weeks interval the completed questionnaire which numbered up to 400 copies were retrieved.

Validity of the Instrument: The questionnaire was subjected to face validation by experts in Educational Measurement and a Senior lecturer of Educational Research and Statistics all of the University of Cross River State, (UNICROSS), Calabar. These experts scrutinized the relevance of the items in the instrument to the work, suitability of the number of items and appropriateness of the instrument in general to the purpose of the study and made useful correction.

Method of data analysis: The research questions were answered using means score and standard deviations, while the hypotheses were tested using Simple linear regression analysis statistical tool at alpha level of 0.05.

RESULTS AND DISCUSSION

Table 1: The result in table 1 shows that there were 200 (50.0%) males and 200 (50.0%) females.

Demographic Description of Study Sample

Variable Name	Category	N	%
Gender	Male	200	50.0
	Female	200	50.0
	Total	**400**	**100.0**

The result in table 1 shows that there were 200 (50.0%) males and 200 (50.0%) females. Hence, the sample was considered heterogeneous enough for the study.

Table 2: showed that freshmen's adaptation to social activities has the highest mean score than freshmen's adaptation to social relationship

Descriptive Statistics of Study Variables by Gender

Variable Name	n		S.d	Sd. Error	Minimum	Maximum
Educators' lack of knowledge and expertise regarding cyberspace	400	4.7156	.45216 .	.03014	3.00	4.00
Cyber security knowledge in data management	400	4.2844	45216	.03014	3.00	4.00
Gender	400	2.5644	.49694	.03313	1.00	2.00

Educators' lack of knowledge and expertise regarding cyberspace in tertiary institutions has the highest mean score of (x.=4.7156) followed by Cyber security knowledge in data management in tertiary institutions with the mean score of (x=4.2844) and Gender (male and female students) has the least mean score of (x=2.5644).

Data in Table 3 Shows Regression of significant influence of cyber security knowledge in data management in tertiary institutions by the educators' lack of knowledge

R-value = .022[a] Adj. R-squared = -.003
R-squared= .002 Standard error = .29760

Source of Variation	**Sum of squares**	**Df**	**Mean square**	**f-value**	**p-value**
Regression	.099	1	.099	.298	229[b]
Residual	25.217	399	.248		
Total	25.316	400			

Predictor Variable	Unstandardized coefficient		Standard coefficient	t-value	p-value
		Std. error			
Constant	2.392	.275		2.058	.000
The educators' lack of knowledge and expertise regarding cyberspace	.026	.074	.022	.431	.229

* Significant at .05 level.

The result in Table 3 shows that an r-value of .022[a] was obtained giving an r-squared value of .002. This means that about 2% of the total variance in cyber security knowledge in data management in tertiary institutions is explained by the variation in the educators' lack of knowledge and expertise regarding cyberspace in tertiary institution. The p-value (.000) associated with the computed f-value (.298) is less than .0.5. Hence, the null hypothesis was rejected, this means that there is a significant influence of freshmen's adaptation to social activities in tertiary institution on their manifest anxiety and their academic achievement, with both regression constant (2.392) and coefficient (.022) making significant contribution in the prediction model (t=2.058 & .431 respectively, P=.000≤.05).

Table 4 showed that Cyber security knowledge in data managementin tertiary institution does not significantly reduces cyber-bully, online fraud, racial abuse, pornography and gambling among educators and students in tertiary institution in Cross River State, Nigeria.

Regression of significant reduction of cyber-bully, online fraud, racial abuse, pornography and gambling among educators by Cyber security knowledge in data management in tertiary institutions.

R-value = 014[a]	Adj. R-squared = -.005
R-squared= .004	Standard error = .59797

Source of Variation	**Sum of squares**	**df**	**Mean square**	**f-value**	**p-value**
Regression	.015	1	.014	.081	.890[b]
Residual	88.298	390	.848		
Total	88.316	400			

Predictor Variable	Unstandardized coefficient		Standard coefficient	t-value	p-value
		Std. error			
Constant	8.612	.083		6.615	. 000
Freshmen's adaptation to social relationship	-.014	.051	-.018	-.166	.890

* Significant at .05 level.

The results in Table 5 show that an r-value of 018[a] was observed, giving an r-squared value of .000. This means that about 4% of the total variance in reduction in cyber-bully, online fraud, racial abuse, pornography and gambling among educators is explained by the variation in Cyber security knowledge in data managementin tertiary institution. The p-value (.000) associated with the computed f-value (.081) is less than .05. As a result, the null hypothesis was rejected. This means that there is a significant freshmen's adaptation to social relationship in tertiary institution predicts their manifest anxiety and their academic achievement. With both the regression constant (8.612) and coefficient (-.018) making significant contribution in the prediction model (t=6.615 and -.166 respectively, P=.000 ≤.05).

Discussion of findings

The results of this study shows that the educators' lack of knowledge and expertise regarding cyberspace in tertiary institutions significantly influence cyber security knowledge in data management in tertiary institutions and Cyber security knowledge in data management in tertiary institutions significantly reduces cyber-bully, online fraud, racial abuse, pornography and gambling among educators and students in tertiary institutions in Cross River State, Nigeria.

Evans, Maglaras, He, and Janicke, (2016). Study Human Behaviour as an aspect of Cyber security Assurance. The study found out as stated by experts and policy makers, the frequency and severity of cyber-attacks is anticipated to continue rising and venturing into areas that were not prime targets in the past, such as academic data. Personal data has always

been targeted by hackers because of the value attached to it by marketing institutions and the field of social engineering. Most of the information is accessible to devices that are connected to the World Wide Web via the Internet. As such, it is imperative that the developers of such websites must have sufficient experience to manage.

Rahman, Sairi, Zizi, and Khalid (2020) study on the Importance of Cyber security Education in School observed that despite the fact that the Internet has positively impacted people's lives, there are negative issues emerged related to the use of Internet. Cases like cyber-bully, online fraud, racial abuse, pornography and gambling had increased tremendously due to the lack of awareness and self-mechanism among Internet users to protect themselves from being victims to these acts. However, past research revealed that the level of awareness among Internet users is still low or moderate. One of the vital measures to be taken is to cultivate knowledge and awareness among Internet users from their early age, i.e., young children. Young children specific all educated to operate in a safe manner in cyberspace and to protect themselves in the process. The objective of this systematic review paper is to explore why it is so critical that modern learners are educated about the risks associated with being active in cyberspace and the strategies that stakeholders can use to promote cyber security education in schools. In this paper, few strategies are discussed as how cyber security education can be implemented in schools.

Alzighaibi (2021) study Cyber security Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment. The study found out that proprietary knowledge, complex equipment designs and blueprintsfor yet to be patented products has all become extremely susceptible tocyber security attacks. This research will investigate factors that affect that mayhave an influence on perceived ease of use of cyber security, the influence ofperceived ease of use on the attitude towards using cyber security, the influenceof attitude towards using cyber security on the actual use of cyber securityand the influences of job positions on perceived ease of use of cyber securityand on the attitude towards using cyber security and on the actual use ofcyber security. A model was constructed to investigate eight hypotheses thatare related to the investigation. An online questionnaire was constructed tocollect data and results showed that hypotheses 1 to 7 influence were significant.However, hypothesis 8 turned out to be insignificant and no influencewas found between job positions and the actual use of cyber security.

Bologa, Lupu, Boja, and Georgescu, (2016) study Sustaining Employability as a process for Introducing Cloud Computing, Big Data, Social Networks, Mobile Programming and Cyber security into Academic Curricula sustainability. The study shows that Technology (ICT) has resulted in significant challenges to data security.The demanding matter of privacy when choosing a technology platform to adopt as an institution remains paramount, in addition to the consent of the platform owners to the option chosen.

Carin, Cybenko, and Hughes, (2018) study on Cyber security Strategies and Methodology maintained that Computer Social media platforms including Facebook, Twitter, Instagram and Google among others have had challenges in the compliance of privacy and data security laws of other countries in the European Union as well as Australia. This means that data results in surveillance, breach, and governments as well as private institutions polices deregulation should strive to ensure the safety and integrity of their data.

Evans, Maglaras, He, and Janicke, (2016). Study Human Behaviour as an aspect of Cyber security Assurance. The study found out as stated by experts and policy makers, the frequency and severity of cyber-attacks is anticipated to continue rising and venturing into areas that were not prime targets in the past, such as academic data. Personal data has always

been targeted by hackers because of the value attached to it by marketing institutions and the field of social engineering. Most of the information is accessible to devices that are connected to the World Wide Web via the Internet. As such, it is imperative that the developers of such websites must have sufficient experience to manage.

Implication for Educational Management in Nigeria.

The following are the implication ofdigitalizing cyber security for data management is as follows;
1. The implication of this study to educational managers in Nigeria is that it may encourages them to advance themselves in technological development since it is gradually affecting their jobs especially in data management, students and educational records keeping.

2. Most educators lack knowledge and expertise regarding cyberspace and cyber security for data managementin schools. This study may educate them on issues of regarding cyberspace and cyber security for data managementin schools.

2. Higher institutions and government ministries in Nigeria are also lacking resources and facilities to implement cyber security education. This study may be used as a reference materials for the improvement of cyberspace and cyber security for data managementin schools.

Conclusion and recommendations

The study concludes that the educators' lack of knowledge and expertise regarding cyberspace in tertiary institutions significantly influence cyber security knowledge in data management in tertiary institutions and Cyber security knowledge in data management in tertiary institutions also significantly reduces cyber-bully, online fraud, racial abuse, pornography and gambling among educators and students in tertiary institutions in Cross River State, Nigeria. Based on the conclusion, it was recommended that tertiary institutions management should formulate educational policies and curriculum that will help in addressing problems of cybercrime in schools. And students and educators should learn Cyberspace knowledge since it is very important in their day to day activities.

References

Alzighaibi, A.R. (2021) Cybersecurity Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment. Journal of Computer and Communications, 9, 77-90. https://doi.org/10.4236/jcc.2021.911006. Received: September 29, 2023.

Anekwe, J. U (2017).Impact of Virtual Classroom Learning on Students' Of Nigerian Federal And State Universities;*European Journal of Research and Reflection in Educational Sciences* , 5(3),1-16

Bennett, S., Myatt, M., Jolley, D., & Radalowicz, A. (2001). *Data Management for Surveys and Trials. A Practical Primer Using EpiData*. The EpiData Documentation Project. Available:www.epidata.dk/downloads/dmepidata.pdf.

Bologa, R., Lupu, A.R., Boja, C. and Georgescu, T. (2016) Sustaining Employability: A Process for Introducing Cloud Computing, Big Data, Social Networks, Mobile

Programming and Cybersecurity into Academic Curricula. Sustainability , 9, Article No. 2235. https://doi.org/10.3390/su9122235

Carin, L., Cybenko, G. and Hughes, J. (2018) Cybersecurity Strategies: The QuERIES Methodology. Computer , 41, 20-26. https://doi.org/10.1109/MC.2008.295

Evans, M., Maglaras, L.A., He, Y. and Janicke, H. (2016). Human Behaviour as an Aspect of Cybersecurity Assurance. Security and Communication Networks, 9, 4667-4679. https://doi.org/10.1002/sec.1657

Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F (2020) The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology, Vol. 10, No. 5, p*379.

http://www.theguardian.com/public-leaders-network/2014/apr/15/big-data-open-data-transform-government. Accessed 10 October 2014.