NAU Journal of Technology & Vocational Education, Vol. 9, No. 1, July 2024

ADOPTION OF DEVICE MANAGEMENT POLICIES AS TECHNIQUE FOR FRAUD PREVENTION BY MANAGEMENT STAFF IN TERTIARY INSTITUTIONS IN BAUCHI STATE

C. C. Okolocha [1] & Cecilia Ifesi[2]
[1,2] Department of Technology and Voctional Education, Nnamdi Azikiwe University Awka, Agbor
estherfavour27@gmail.com

Abstract
This study ascertained adoption of device management policies as technique for fraud prevention in tertiary institutions in Bauchi State. One research question guided the study and one null hypothesis was tested. Descriptive survey research design was adopted for the study. The population comprised 696 management staff working in the six public tertiary institutions in Bauchi State. No sample was used because the population size was manageable for the researcher. A 13-items structured questionnaire was used. The instrument was validated by three experts. To determine the internal consistency of the items, Cronbach Alpha was used to determine the reliability co-efficient value of 0.79. Mean and standard deviation were used to answer the research questions, while Analysis of Variance was used to test the null hypotheses at 0.05 alpha levels. The findings of the study revealed that management staff disagrees on adoption device management policies as technique for fraud prevention in tertiary institutions in Bauchi State. Management staffs' years of working experience do not significantly influence their mean ratings on the adoption of device management policies as technique for fraud prevention in tertiary institutions in Bauchi State. The study concluded that the device management policies as technique in the study are not adopted by management staff for fraud prevention in tertiary institutions in Bauchi State. It was recommended among others that business and office education lecturers should therefore ensure that data security management techniques such as device management policies are taught to their students when teaching about techniques for reducing fraud and are included in their business education curricula for the training of business education in tertiary institutions.
Keywords: Tertiary Institutions, Device Management Policies Techniques, Management Staff, Fraud Prevention.

Introduction

The role of tertiary institutions in a nation's growth and development is universally acknowledged. They are crucial to the growth of a country's human capital. A nation must rely on tertiary institutions to generate highly skilled citizens able to contribute to overall solutions in order to address its socio-cultural, economic, political, scientific, and technical challenges. In Nigeria, tertiary institutions are essential for supporting growth, building shared prosperity, and reducing unemployment and poverty. According to the Federal Republic of Nigeria (FRN), (2013), tertiary institutions are the driving force behind social and economic development, and both their quantity and, more crucially, their quality, speak volumes about Nigeria's resolve to maintain a competitive edge. Tertiary institutions are the level of education following secondary school. They are also known as higher education, tertiary education, third stage, and post-secondary education. Tertiary institutions provide education at universities, colleges of education, polytechnics, and mono-technics, including those that offer correspondence courses. Tertiary institutions in Nigeria face numerous challenges in their efforts to provide quality education to

the Nigerian populace. Some of these challenges include; poor funding, poor teaching and learning facilities, inadequate manpower and most especially fraud. Fraud is the misuse of position for one's own benefit. According to PricewaterhouseCoopers (PwC) (2016) stated that fraud is any act or omission, including a misrepresentation, that intentionally or recklessly attempts to deceive a person in order to receive an advantage, whether it be monetary or otherwise, or in order to escape an obligation. According to Okoye, Sabastian, Yohana, and Rauta (2017), fraud takes the form of financial statement fraud, asset theft, and corruption. Customer fraud, cybercrime, asset misappropriation (financial and non-monetary) and bribery and corruption were classified as frequent fraud (Okoye, et al.).

In Nigeria, fraud is rampant in every industry, including banking, healthcare, energy, housing and education (Okoye, Sabastian, Yohana and Rauta, 2017). In both public and private sectors, fraud is so pervasive that it has become the norm. Fraud has also slowed the expansion of Nigeria's education delivery. An education system plagued by fraud is likely to produce dishonest public officials, incompetent leaders, inexperienced instructors, quack physicians, technologists and technicians (Ile and Odimmega, 2018). The majority of Nigeria's educational institutions do not appear to understand how fraud affects their ability to maintain financial stability and builds public distrust. In light of this, Ile and Odimmega further noted that fraud was committed by management staff of tertiary institutions such as administrators, directors, managers, leaders and supervisors, team leaders, and anyone else acting in a leadership capacity. Both academic and non-academic employees, such as lecturers, senior staff, staff members of alumni offices, staff members of the bursary/treasury, staff members of institution project centers, public relations units, and other revenue-generating departments, are capable of committing fraud. Management staff are also officials, directors, and administrators includes; improper contract awarding, misappropriation of funds, admissions offered on the basis of financial need, and diverting research grants or other funds designated for projects into personal accounts.

In an attempt to arrest increasing cases of fraud in Nigerian tertiary institutions, the management staff of the institutions needs to play a crucial role in the prevention of fraud by setting up and maintaining proper internal control systems that can offer security and accountability for the data entrusted to them. They are also required to understand the dangers and exposures associated with the vast amounts of frequently private data that tertiary institutions gather and disseminate. Due in large part to improvements in technology, expansion of communication, the internet and the cost of data storage, the amount of data being stored in tertiary institutions is increasing exponentially (Lewal, 2017). However, as data generation grows, so does the risk of data loss that Nigerian tertiary institutions must contend with. Because of the internet's rapid expansion, tertiary institutions may leave a lot of data footprints that give cybercriminals access to the institution's websites to gather information for their fraudulent schemes. Onaleye (2021) observed that despite the existence of the Nigeria Data Protection Regulation (NDPR) (2019), educational institutions and agencies in Nigeria, including the National Examination Council (NECO), Joint Admission and Matriculation Board (JAMB) and Gombe State University have reported data breaches, and have had to pay expensive repair costs in addition to fines and a general decline in public trust. Knoblauch (2017) noted that cybercriminals are now routinely targeting educational institutions in Nigeria. Song (2019) claimed that the Nigerian education sector was responsible for 13 percent of the data breaches that occurred in the first half of 2017 that led to the compromising of 32 million records.

Data is the term used to describe information that is created and electronically (in a computer system) or manually (on files) stored. International Data Corporation (2016) defined

data as letters, symbols, and binary that a computer uses to carry out activities. Data may be stored or sent as electronic signals on any device or in any format. Data are assets to tertiary institutions. An institution may be the owner of the data it has, or it may be the custodian of data owned by another organization. Tertiary institutions provide a variety of data, including data on staff and students, data on healthcare (medical records and laboratory tests), and data on finances (Biddle, 2017). In order to safeguard data from the hazards of data breaches, Knoblauch (2017) claimed that data security has grown to be one of the most urgent security concerns for management and employees of tertiary institutions.

Data security basically refers to preventing unwanted access to and corruption of data. It is a procedure for safeguarding data against damaging elements and unlawful access. Data security, according to the Alimba (2018), is the process of defending digital data against unauthorized access, corruption, or theft across the course of data's entire lifecycle. Strong data security guarantees that crucial information for tertiary institutions is backed up and accessible should the main source become unavailable. If the institution's data include any personally identifiable information that must be properly handled to comply with the Nigeria Data Protection Regulation (NDPR), security becomes even more crucial. Data security is a component of electronic records management. It is an important phase in the electronic records management life cycle.

Data management is the creation and implementation of strategies, policies, and practices that manage, safeguard, deliver, and enhance the value of data. The primary goals of electronic records management, according to Oko, Egba, Egba, Achimugu and Achimugu (2016), are to guarantee proper data storage, data security, and data retrieval whenever necessary. Office Technology and Management (OTM) departments teach data security management as a part of office application in Nigerian universities and polytechnics. Office application seeks to equip OTM students with office skills using a keyboard as an input device, working with computer excel, word processing, reprographics for documentation, office practice skills, and database administration among others (Bupo, 2016). OTM is a field of business education that gives students the knowledge and skills for data management (Oladunjoye, 2016).

Due to the fact that data security is crucial for preventing fraud in tertiary institutions, institutions need to create security procedures to safeguard their data all the way through its life cycle (NDPR, 2019). In accord, Unini (2019) noted that education institutions must make sure that all data are safeguarded from loss or unauthorized users in order to ensure operational efficiency and consistently match the expectations of the teeming public. Additionally, tertiary institutions must make sure that they fulfill their obligations honestly and without engaging in dishonest behaviour. However, Babatunde (2020) reported that there were documented instances of fraud in the educational system, and significant issues about its causes and prevention methods yet remain unsolved. The loss of data in tertiary institutions, could compromise people's privacy and expose sensitive information to the public. Additionally, it might make it harder for tertiary institution administrators to assign blame for staff members' acts and hold them accountable.

The process of assuring the identification of the source or sender of data, the integrity of the data, and the control of the identity of the destination or receiver is referred to as data security management (Ofori-Duodu, 2019). Tertiary institutions can use several data security management techniques to prevent fraud. Data security management techniques include the installation of firewalls, the use of data encryption technologies, the development of organizational policies for handling sensitive or confidential data, the protection of e-mailing systems, and the continual development of staff data security skills (NDPR, 2019). Data security compliance monitoring and data security auditing were identified as techniques for securing data

for fraud prevention (Michael, 2020). Multiple-security-technology solutions, data security policies, device management policies, and data classification was proposed by (Al-Edwan, 2016). However, the adoption of device management policies as technique for fraud prevention by management staff in tertiary institutions is evaluated in this study.

To lock codes and passwords, device management policies mandate complete disk encryption to safeguard data on the device, permit remote data wipes, and restrict users from installing unapproved apps (Oni, 2016). They also mandate remote data wipes and device tracking. An essential data management approach that might guarantee the security of data in tertiary institutions and reduce the likelihood of fraud is routine data security auditing. This technique entails evaluating the information systems within and across institutions and determining what needs to be improved. Alawaqleh (2021) stated that fraud management practices have positive and significant effect on bank efficiency and operational performance of the selected deposit money banks. Adelola, Dawson and Batmaz (2015) revealed that most deposit money banks in Nigeria have experienced declined in non-financial performances due to poor fraud management practices which have resulted in financial losses to banks and loss of public confidence in the banking sector. Agyemang (2020) reported that respondents agreed that management ensure that all necessary measures needed to prevent and detect fraud are provided. Oladunjoye (2016) noted that experienced managers have over the years developed effective techniques for securing destruction in their organizations' data when compared with the less experienced managers. In order to prevent fraudsters from accessing their data, management of tertiary institutions must work with management staff that handles day-to-day data management tasks to audit their IT infrastructure, including their computers, networks, and mobile devices. The management staff could benefit from this partnership.

Management staff are individuals who are in charge of overseeing the work of others, and include administrators, directors, managers, leaders and supervisors, team leaders, and anyone else acting in a leadership capacity. Management staffs are indispensible employees in public tertiary institutions as they ensure that new innovations are implemented in tertiary institutions. They also work to ensure smooth operations of tertiary institutions and set up internal control systems to prevent fraud occurring in their tertiary institutions. In view of this, the management staff ensures that staffs that handle data management tasks such as data documentation, organizing, managing data, managing inventory of assets and supplies, coordinating between data of departments and operating units perform their functions diligently to mistakes that will lead to data breach (Babatunde, 2020). The management staff could be individuals with different educational qualifications and working experiences, and are expected to possess competencies required to adopt data security management techniques for prevention of fraud in their offices.

Management staff members must implement suitable data security management strategies. However, problems with financial scandals, corruption, purposeful data destruction after misappropriation of funds to cover up the case, ongoing data loss by staff, and hacking of crucial information (data) of both the federal and state tertiary institutions in Nigeria suggest that these techniques are not widely adopted for fraud prevention. Management staff with 11 years and above working experience could be adopting data security management techniques on account of having attended more trainings and re-training programmes, workshops, data security summits and other data security management programmes within and outside the country than staff with 1-5 years, and those with 6-10 years working experience. It could also be that experienced management staff possess more data security management techniques as the case may be compared to less experienced ones. Oladunjoye (2016) in agreement observed that

experienced managers have over the years developed effective techniques for securing their organizations' data when compared with the less experienced managers. This could be attributed to exposure to different data security management techniques during course of learning. Generally, management staff embark on more training and development programmes to up-date their knowledge and skills and to improve on their jobs. In view of the high rate at which fraud is being perpetuated in tertiary institutions in Nigeria, there is need for this study to ascertain the adoption of device management policies as technique for fraud prevention by management staff in tertiary institutions in Bauchi State.

Statement of the Problem

There are many data security management techniques that tertiary institutions in Nigeria can adopt to reduce the likelihood of fraud. However, the evidence that is now available indicates that some tertiary institutions in Nigeria, including those in Bauchi State, have embraced some of these techniques, including data mining, the use of passwords, activating fire walls, utilizing antivirus and antispyware, and the use of secure records scanning. As indicated by the daily reports of data theft, loss, and damages that continue to expose the private data of tertiary institutions to the public, it appears that management staff may not be adopting most of these tactics in order to secure data in their offices. The researcher is worried that the inability of management staff of tertiary institutions in Nigeria, especially in Bauchi State to adopt of device management policies as technique will worsen the incidence of data privacy breaches that expose the institutions' confidential information to the general public, therefore giving cyber criminals opportunity to hack into the institutions' database to carry out fraud. Management staff could also make it impossible to prevent fraud in tertiary institutions which are increasingly committed through computer database. However, the adoption of adoption of device management policies as technique for fraud prevention by management staff in tertiary institutions in Bauchi State seems not to be revealing. Hence, this study is imperative as it will reveal the adoption of device management policies as technique by management staff of tertiary institutions technique for fraud prevention in Bauchi State.

Research Questions

One following research question guided this study:

1. What is the device management policies as technique for fraud prevention by management staff in tertiary institutions in Bauchi State?

Hypotheses

The following null hypotheses were tested at 0.05 level of significance:

1. There is no significant difference in the mean ratings of management staff on the device management policies as technique for fraud prevention in tertiary institutions in Bauchi State based on their years of working experience.

Method

The study adopted descriptive survey design. The population of the study comprised 696 management staff working in the six public tertiary institutions in Bauchi State, Nigeria. All the 696 management staff working in the six public tertiary institutions in Bauchi State was used because the population sample is small. Data for this study was collected using a 13 items structured questionnaire. The respondents were requested to rate the items on a 5-point rating scale of Strongly Agree (SA), Agree (A), Undecided (U), Disagree (D) and Strongly Disagree (SD) with values 5, 4, 3, 2 and 1 respectively. The instrument was validated by two experts in

business education. Cronbach Alpha method was used to establish the reliability of the instrument. The reliability coefficients values of 0.79. Out of the 696 copies of the questionnaire distributed to the respondents in their organizations through direct approach which facilitated a response rate, 687 copies (representing 99 percent) were retrieved with an attrition rate of 12 copies (representing 1 percent) and used for data analysis. Data collected were analyzed using mean and standard deviation to answer research questions while ANOVA was used to test the null hypotheses at 0.05 level of significance. The application of Statistical Package for Social Sciences (SPSS) version 23 was used for data analysis. For the hypotheses, p-value was used for decision making. Where the calculated p-value is less than the stipulated level of significance 0.05 ($p < 0.05$), it implies that there is a significant difference between respondents' mean scores and the null hypothesis is rejected. On the other hand, if the p-value is greater than or equal to the alpha level of 0.05 ($p \geq 0.05$), it means that there is no significant difference in the respondents mean scores and is not rejected.

Result

Research Question 1. What is the device management policies adopted as techniques for fraud prevention by management staff in tertiary institutions in Bauchi State?

Table 1: Management staffs' mean ratings of device management policies adopted as techniques for fraud prevention in tertiary institutions in Bauchi State. N =687

S/N	Device management policies adopted as techniques for fraud prevention	$\overline{X}$	SD	Remarks
1.	Protecting office computers with passwords	4.33	0.53	Agree
2.	Using office computers to watch movies	1.58	0.79	Disagree
3.	Using my office computers for social media (Whatsapp, Facebook) activities	1.54	0.82	Disagree
4.	Sharing office computer passwords with other colleagues	2.24	0.68	Disagree
5.	Being responsible for the loss of data in office computer	4.20	0.54	Agree
6.	Installing applications in office computers without authorization	2.28	0.63	Disagree
7.	Opening e-mail messages without first scanning them	1.61	0.78	Disagree
8.	Using office computers to download applications over the internet	1.54	0.82	Disagree
9.	Connecting office computer to internet through only a secure wireless network	4.20	0.54	Agree
10.	Loading pirated software or illegal content into office computers	1.68	0.74	Disagree
11.	Connecting only scanned and certified virus free USB drives (flash drive, external hard disk, memory card) to office computer	3.61	0.56	Agree
12.	Using office computers to send and receive private e-mail messages	1.61	0.78	Disagree
13.	Reporting all lost/stolen office devices to supervisor immediately	1.72	0.70	Disagree

Grand Mean	**2.47**	**Disagree**

Data in Table 1 show that the item-by-item analysis reveals that out of 13 items listed. Four of the items have mean score that ranging from 3.61 to 4.33 indicating agrees and the remaining five items disagree with mean scores ranging from 2.54 to 2.28. The standard deviations of 0.53 to 0.82 show that the respondents are not wide apart in their mean ratings. The grand mean scores of 3.61 shows that, on the whole, management staff in the area of the study disagreed that they adopt device management policies as techniques for fraud prevention in tertiary institutions in Bauchi State.

Hypothesis 1. There is no significant difference in the mean ratings of management staff on the adoption of device management policies as techniques for fraud prevention in tertiary institutions in Bauchi State based on years of working experience (1-5 years, 6-10 years or 11 years and above).

Table 2: Summary of Analysis of Variance on the mean ratings of management staff on the adoption of device management policies adopted as techniques for fraud prevention in tertiary institutions in Bauchi State based on their years of working experience (1-5 years, 6-10 years or 11 years and above).

	Sum of Squares	df	Mean Square	F	P-value	Remarks
Between Groups	288.575	2	144.287	10.731	.091	Not Significant
Within Groups	3146.438	684	13.446			
Total	3435.013	686				

As shown in Table 2, the F-ratio (df: 2/684) is 10.731 and the P-value (.091) is greater than the stipulated 0.05 level of significance (P-value > alpha level). It was therefore noted that there is no significant difference in the mean ratings of management staff on the adoption of device management policies as techniques for fraud prevention in tertiary institutions in Bauchi State based on their years of working experience. Therefore, the null hypothesis is not rejected.

Discussion of Findings

Findings of the study revealed that management staff in the area of the study disagreed that they adopt device management policies as techniques for fraud prevention in tertiary institutions in Bauchi State. This implies that they are enable to lock codes and passwords to safeguard data on the device, permit remote data wipes, and restrict users from installing unapproved apps in their institution. This finding is in line with Alawaqleh (2021) who stated that fraud management practices have positive and significant effect on bank efficiency and operational performance of the selected deposit money banks. Adelola, et-al revealed that most deposit money banks in Nigeria have experienced declined in non-financial performances due to poor fraud management practices which have resulted in financial losses to banks and loss of public confidence in the banking sector. The findings disagrees with Agyemang (2020) reported that respondents agreed that management ensure that all necessary measures needed to prevent and detect fraud are provided.

The findings of the study further revealed there is no significant difference in the mean ratings on management staffs on the device management policies as techniques adopted for fraud

prevention in tertiary institutions in Bauchi State based on educational qualification and years of working experience. This finding agrees with Oladunjoye (2016) who revealed that experienced managers have over the years developed effective techniques for securing destruction in their organizations' data when compared with the less experienced managers. The reason for the similarities in test of hypotheses is because they are mandated to use remote data wipes and device tracking in their institution. The reason for determining management staff adoption of data security management techniques for fraud prevention in tertiary institution is because they are in a better position to indicate whether they adopt device management policies as techniques for fraud prevention in their offices.

Conclusion

Based on the findings of the study, it is concluded that the device management policies as technique in the study are not adopted by management staff for fraud prevention in tertiary institutions in Bauchi State.

Recommendations

Based on the findings and conclusion of the study, the following recommendations are made:

1. Business and office education lecturers should therefore ensure that data security management techniques such as device management policies are taught to their students when teaching about techniques for reducing fraud and are included in their business education curricula for the training of business education in tertiary institutions.
2. Society through the government should organize on-going seminars and workshops to re-educate management staffs on relevant of adoption of data security management techniques for fraud prevention in tertiary institutions.

References

Adelola, T., Dawson, R. and Batmaz, F. (2015). Nigerians' perceptions of personal data protection and privacy. *International Research Journal of Engineering and Technology (IRJET), 6*(1). 137-144.

Al-Edwan Z.S. (2016). The security education concepts in the textbooks of the national and civic education of the primary stage in Jordan: An analytical study. *International Education Studies, 9*(9), 146-156.

Alimba C. N. (2018). Security and security measures for schools operating in domains prone to insurgency in Nigeria. *International Journal of Public Administration and Management Research (IJPAMR), 4*(3), 36-48.

Alshaikh, M., Maynard, S. B. Ahmad, A. and Chang, S. (2018). *An exploratory study of current information security training and awareness practices in organizations.* Proceedings of the 51st Hawaii International Conference on System Sciences, 12th -15th September, 2018.

Babatunde, E. M. (2020). Fraud management and institutional performance of federal tertiary institutions workers in Nigeria. *International Journal of Innovative Research and Advanced Studies (IJIRAS), 7*(6), 309-313.

Biddle, S. (2017). Building security forces & stabilizing nations: The problem of agency. *Daedalus, the Journal of the American Academy of Arts & Sciences, 14*(6), 126-138.

Bupo, O. G. (2016). Availability and awareness of financing opportunities for small scale entrepreneurs in Rumuepirikom communities, Port Harcourt. *Association of Business Educators of Nigeria Conference Proceedings, 3*(1), 721-727.

Federal Republic of Nigeria (2013). National Policy on Education (6th Ed.). NERDC Press. Fredericks, K. A., McComas, R. E. & Weatherby, G. A. (2016). White collar crime: recidivism, deterrence, and social impact. *Forensic Research Criminology International Journal*, *2*(1), 5-14. DOI: 10.15406/frcij.2016.02.00039.

Ile, C. M. and Odimmega, C. G. (2018). Use of forensic accounting techniques in the detection of fraud in tertiary institutions in Anambra State, Nigeria. *African Research Review. International Multi-Disciplinary Journal, 12*(1), 66-76.

Knoblauch, D. (2017) European Security Certification Framework deliverable 2.2 Continuous Auditing Certification Scheme Retrieved from: https://cdn0.scrvt.com/fokus/1edfbe2d5ab52e28/e2dd1ac7870b/ D2.2-Continuous_auditing_certification_scheme_V1.pdf

Lawal, I. (2017). A nation weighed down by certificate scandals. https://guardian.ng/features/a-nation-weighed-down-by-certificate-scandals/

Michael, H. (2020). *Exploring cyber security awareness and training strategies to protect information systems and data.* Doctoral Thesis submitted to College of Management and Technology, Walden University.

Nigerian Data Protection Regulation (NDPR), (2019). Implementation framework. Same sex marriage (Prohibition) Act, 2019.

Ofori-Duodu, M. S. (2019). *Exploring data security management strategies for preventing data breaches*. Unpublished Ph.D Dissertation submitted to the College of Management and Technology, Walden University.

Okoye, E. I., Maimako, S. S Jugu, Y. G. and Jat, R. B. (2017) *Principles of fraud investigation on and forensic accounting.* Awka: SCA Heritage Nigeria Ltd.

Oko, M. C., Egba, A. U., Egba, E. I., Achimugu, O. and Achimugu, P. (2016). Improving data handling in Nigerian tertiary institutions through effective electronic record management. *Indian Journal of Science and Technology*, *9*(46), 1-5.

Oladunjoye, T. G. (2016). Optimizing business education for national development. *Nigerian Journal of Business Education (NIGJBED), 3*(1), 1-16. Retrieved from http://www.nigjbed.com.ng.

Onaleye, T (2021). Jamb isn't the first! here are 10 times Nigerian government agencies have Been Hacked in the Last Decade. https://technext.ng/2021/04/15/jamb-isnt-the-first-here-are-10-times-nigerian-govt-agencies-have-been-hacked-in-the-last-decade/

Oni, J.A. (2016). *Combating security challenges in the University system, ANUPA 2016.* University of Lagos. Nigeria.

PricewaterhouseCoopers (PwC) (2016). PwC Nigeria transparency report 2016. https://www.pwc.com/ng/en/assets/pdf/transparency-report-2016.pdf

Song, V. (2019). Mother of all breaches exposes 773 Million Emails, 21 Million Passwords. Gizmodo.

Unini, C. (2019). UBA server hacked, flour mills' N752m stolen, bank's auditor tells court. https://thenigerialawyer.com/uba-server-hacked-flour-mills-n752m-stolen-banks-auditor-tells-court/