MPRI-JAIMR | INTERNATIONAL JOURNAL OF AFRICAN INNOVATION & MULTIDSCIPLINARY RES.
VOL. 1 NO. 1 JUN-2022

AVOIDING CONFIDENTIAL INFORMATION LEAKAGE IN ORGANIZATIONS FOR SUSTAINABLE DEVELOPMENT

OGHOMWEN, JOHN N. SMITH; KOLO JOSHUA; MOHAMMED SAIDU KPAKI; & SALAKO MORENIKEJI MEDINAT

Department of Office Technology and Management, the Federal Polytechnic, P.M.B. 55, Bida- Niger State.

Abstract

This study examined ways of avoiding confidential information leakage in organizations for sustainable development in Abuja metropolis. The study adopted the survey research design. The population of the study consisted of fifty (50) IT staff in the organizations purposively selected for the study. The whole population of fifty was used as sample for the study. The instrument for data collection was a 24-items questionnaire. The analysis of data was done using mean and standard deviation. The findings revealed amongst others that human and technology related leakages could be avoided by the selected organizations by paying ICT Staff and other staff associated with information sharing enhanced salaries and peculiar allowances, provide ICT staff security training regularly, using paper shredders, limit employees access to confidential information, holding ICT staff accountable, encrypting files and data base, use of password and locking down networks. It was therefore recommended amongst others that business organizations should implement security measures such as the use of password, paper shredders, provide security training for ICT staff, limit employees access to confidential information and holding ICT staff accountable for breaches of confidential information in the organizations to ensure sustainability of business.

KEYWORDS: *confidential information, information leakage, intentional leakage, unintentional leakage, sustainable development.*

EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

Introduction

Information is the life wire of any organization be it public or private. The role of information in any organization is great. Information helps business in decision making process which gives companies an edge in the competitive environment. Information itself is a corporate resource which is the sole product of the office. Confidential information is top secret data or sensitive documents which guide companies on their daily operations. It can also be referred to as those official issues with paramount importance to business organizations and because of its importance, it should be seen as the life wire of business and should be kept away from the limelight of the general public (Morshed et al, 2021.

Leakage of confidential information has remained un-rectified factor in business organizations and professional offices. The means and channels through which this information gets to the public is a source of worries to all stakeholders and this is because important files and figures are exposed to those who are not supposed to have access to them (Alneyadi, 2016).

The effects of information leakages could be very detrimental and damaging to organizations. There have been instances where organizations documents were hacked and vital confidential information carted away there by rendering such organizations incapacitated. Leakages which are believed to be caused intentionally and unintentionally seem not to be on the decrease rather they are on the increase from year to year (Safianu, 2016). The collosal financial loses attributed to the confidential linformation leakages deserves the utmost attention of researchers to have urgent look at ways and means of ameliorating the situation and hence the need for this study.

Statement of the problem

Information is a vital tool for the survival for business organizations. Information is power. It is essential to the success of business growth. Every organization has information that is classified as confidential information. Recently, the leakages of confidential information seem to be on the increase in both private and public organizations all over the world (Safianu, 2016). There are daily reports in both online publications, televisions and print media etc of frightening and gargantuan leakages of confidential information. The consequences of confidential information leakages are enormous and they include loss of business investment, loss of clients, direct financial damage, and deterioration of company's reputation to mention a few. Cyber criminality regarding confidential information leakage is

on the increase and if organizations' sustainability is to be maintained, organizations must put in place some drastic measures that will prevent Information leakage. Hence it has become pertinent to examine ways of prevengting confidential information leakage in business organizations.

Objectives of the study

The general objective of the study was to identify ways of avoiding confidential information leakages in selected organizations in Abuja metropolis for sustainable development. Specifically, the study sought to:

1. Identify the types of confidential information leakages in the selected organizations in Abuja metropolis
2. Identify human related ways of avoiding confidential information leakages in the selected organizations in Abuja metropolis for sustainable development.
3. Identify technology related ways of avoiding confidential information leakages in the Selected organizations in Abuja Metropolis fir sustainable development.

Research questions

The following research questions were formulated to guide the study:

1. What are the types of confidential information leakages in the selected organizations in Abuja metropolis?
2. What are the human related ways of avoiding confidential information leakages in the selected organizations in Abuja metropolis for sustainable development?
3. What are the technology related ways of avoiding confidential information leakages in the selected organizations in Abuja metropolis for sustainable development.

Review of related literature

Concept definitions

Confidentiality is a multi-disciplinary issue. It is a state of keeping or being kept secret or private. Words like secrecy, security, privacy, solitude are often used to describe confidentiality.

Confidentiality involves a set of rules or a promise usually executed through confidentiality agreements that limits access or places restrictions on certain types

of information. In every business organizations, confidentiality is highly regarded as the organizations have information and documents which hold the company at its peak. Therefore every employee iss expected or rather mandated to keep the organizations information or documents confidential.

Confidential information is information disclosed to an individual employee or known to that employee as a consequence of the employee's employment in the company. This information is not generally known outside the company or is protected by law. Confidential information can include information in any form, such as written documents/records or electronic data. Such information includes customer information, company financial account information and payrolls, company research data and records, password and Information Technology related information of the organization, assessments and reports. All these are considered confidential information of an organization and should be kept secret. Pelteret and Ophoff (2016) defined confidential information as having control over and being able to limit access to one's personal information. Many established businesses as well as newly launched global ventures base much of their business on knowledge, information and data some of which are highly confidential. Confidentiality builds trust between business organizations and customers, business owners have the obligation to keep their customers information secured and customers feel happy to patronize the business organizations knowing that their personal information is protected.

Confidential information leakages could occur through intentional or unintentional leakage. Intentional leakage implies premeditated, conscious and willful decision of an employee to harm the business operations of the company. This could happen when employees are offered incentives to leak the organization's confidential information for pecuniary interest or it could be a personal vendetta against the company. The act of malicious insider who exploits information for personal gains is intentional leakage (Nzewanta, 2022).

Unintentional leakage implies accidental. This occurs when an insider accidentally exposes critical business information not meant to be shared with third parties. The accidental insider threat is the potential of an individual who has or had authorized access to an organization's network, system, or data through action or inaction , without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or value of the organization's information (Nzewanta, 2022). Organisations must strive to put in

place measures to counter both intentional and unintentional confidential information leakages for sustainable development.

Succinctly put , Sustainable Development (SD) means development that can be continued either in definitely or for a given period. Mensah, 2019, defined (SD) as development that meets the needs of the current generation without compromising the ability of future generations to meet their needs. It is a development paradigm as well as concept that calls for improving living standard without jeopardizing the earth's ecosystem or causing environmental challenges. It simply means keeping business ongoing for the benefit of humanity Scio-economically.

There are various types of confidential information that ought to be kept confidential in an organization. The privacy of personal information is an important area of focus in today's electronic world, where information can so easily be captured , stored and shared Pelteret and Ophoff (2016).

According to Petelret and Ophoff 2016 and Morshed (2021) asserted the following as some of the types of confidential information found in most organizations:

Managerial Information such as employee disciplinary action and also about broad management actions like planned redundancies or employee relations issues. Some managerial information will become public in due course such as planned redundancies and other information may remain confidential for much longer.

Organizational Information:

Organizational information is also known as business information or trade secrets. This covers anything not in the public domain that helps the organization do its work better or more efficiently. It would therefore include information about operations and recruitment of staff, budgets, cost forecast and customer contract information.

Customer information

Business organizations keep personal information of their customer such as the quantity of goods that customers buy, the amount of money customers have in their account and types of goods that customers buy. All these information need to be secured to avoid unnecessary attack by men of underworld.

Professional information

Professionals like doctors, lawyers, Accountants come across information about individuals or organization through their professional position and often bound by

professional codes of conduct as well as formal legal requirement. For example; Doctors know the details of their patient health conditions and treatment. Lawyers know the details of wills and court cases, some of which may be protected by law. Accountants will know about their client tax, income and profit.

Contracts and Commercial Documents

Some of the most important confidential documents include contracts and other business documents. Confidential documentation must be properly handled and stored to protect both your organization and the third-party.

Most contracts have a confidentiality clause. Your contract with important clients could become void if it fell into the wrong hands. Contracts have a lot of sensitive data such as the cost of the services, and the names of the parties involved. If a competitor got their hands on this document, they could use it to hurt your business or steal your clients.

Yousef (2019), Alneyadi et al (2016), safianu et al (2016), and www.quostar (2020), listed the following as some of the ways of avoiding human related types of confidential information leakages in organizations:

* Providing security training for ICT staff from time to time on the accurate ways to share confidential information.
* Use of paper shredders - one of the surest ways to prevent sensitive information from unwanted viewers is proper destruction, shredding of confidential information.
* Implementing good pay packages and other extrinsic and intrinsic motivation for information and technology staff who have authorized access to company confidential information.
* Implementing a clean desk by making sure that display of sensitive documents on desks are completely avoided.
* Educate users - companies must let their employees know what information is confidential and cannot be shared.
* Providing security training for employees - Employees should constantly be trained and retrained by their employers properly to avoid unintentional transfer of documents to the wrong persons or organizations.

According to Alneyadi. et al (2016), Ritala et al (2016), and Greitzer et al (2019) technology related confidential information leakages could be avoided through the following ways:

* Device control -- Organizations should have security policies in place governing the use of devices at workplace. The policies must cover things like password complexity, download and applications guide lines.
* Adding legal denials to outgoing mails.
* Lockdown of network - employers should lockdown their networks to avoid leakages of confidential information after working hours.
* Encrypting files and data base with the help of electronic gadgets.
* Use of password for all sensitive documents and use of firewalls.
* Maintaining the use of one IT firm.
* Prohibiting the use of unauthorized USB on organization computer.

Research methodology

The study employed survey research design. The study was conducted in Abuja metropolis. The Population for the study was fifty (50) IT Staff which was purposively selected. All the population of 50 IT Staff was used as sample for the study. A modified Likert-type of 4-point scale structured questionnaire containing 24-items was used for the study. The face and content validation of the instrument was done with the assistance of three (3) research experts. The reliability of the study was determined using Pearson Product Moment Correlation (PPMC). A reliability coefficient of 0.76 was obtained which indicated that the instrument was reliable for data collection. The data generated from the questionnaire was analyzed using mean and standard deviation. The rating scale were assigned the following nominal values: Strongl Agreed (SA) 1, Agreed (A)2, Strongly Disagreed (SD) 3, Disagreed (D) 4. Any item with a mean score of 2.50 and above was adjudged to be accepted while any item below 2.50 was adjudged to be rejected.

Presentation and analysis of Data

1: What are the identified types of confidential information leakage in the selected organizations in Abuja metropolis.

Table 1: Mean and Standard deviation computation of respondents on the types of information leakages in the selected organizations in Abuja metropolis

N = 50

S/N.	ITEMS	X	SD	REMARKS
1.	Employees information	2.67	0.57	Accept
2.	Company's financial statement	2.88	0.66	Accept
3.	Company's Budget	2.82	0.78	Accept

EDITOR-IN-CHIEF
Prof. A.I. Mteiye [MALAWI]

4.	Assessment, reports and records	2.95	0.77	Accept
5.	Company's payrolls	2.66	0.45	Accept
6.	Contracts and commercial documents	2.63	0.52	Accept
7.	Customer information	2.58	0.72	Accept

Source: Data 2022

From table 1 above, it was revealed that respondents accepted all the seven items as some types of confidential information leakages that exist in organization organizations. They were employee information record with the following scores(X=2.67 SD=0.57); company Financial statement (X=2.88 SD=0.66); budget documents (X=2.82, SD=0.78); assessment, reports and records (X=2.95SD=0.77); company payroll (X=2.66 SD=0.45); contract investment documents (X=2.63 SD=0.52)and customer information (X 2.67 SD 0.72)

Research Question 2: What are the ways of avoiding human related confidential information leakages in the selected organization in Abuja metropolis for sustainable development?

Table 2 mean and standard deviation computation of human related confidential information leakages in the selected organizations Abuja metropolis sustainable development.

N = 50

S/N.	ITEMS	X	SD	REMARKS
1.	Paying ICT Employees good salaries and allowances to discourage them from stealing and trading confidential information	2.56	0.56	Accepted
2.	Providing security training to ICT staff on how to share confidential information	2.88	0.67	Accepted
3.	Using paper shredders to destroy vital documents.	2.98	0.56	Accepted
4.	Maintaining the use of one IT firm.	2.79	0.64	Accepted
5.	Holding the firm or ICT staff accountable.	2.60	0.72	Accepted
6.	Policy of clean desk prohibiting staff from displaying confidential information on their tables.	2.52	0.60	Accepted

7.	Prohibiting the use of personal USB on organization computer.	2.75	0.86	Accepted
8.	Prohibiting the use of personal handset in workplace.	2.66	0.48	Accepted

Source: Data 2022

From the eight (8) items listed as human related ways of avoiding confidential information leakages, all of them were accepted by the respondents. The items were paying enhanced salaries to IT staff (X=2.56 SD=056); training and retraining of IT staff (X=2.88 SD=067); using shredders to destroy vital documents not required (X=2.98SD=0.56); maintaining the use of one IT firm(X=2.79 SD=0.64); Holding the IT staff accountable for any confidential information leakage (X=2.60 SD=0.72). Adopting the policy of clean desk prohibiting staff from displaying confidential information on their table (2.52 SD=0.60); Prohibiting the use of personal USB on organization computer (X=2.75SD=0.86); Prohibiting the use of personal handset in workplace (2.66 SD=0.48).

Research Question 3: What are the ways of avoiding technology related confidential information leakages in the selected organizations in Abuja metropolis sustainable development?.

Table 3 mean and standard deviation computation of Technology related confidential information leakages in the selected organizations Abuja metropolis sustainable development.

N = 50

S/N.	ITEMS	X	SD	REMARKS
1.	Encrypting files and data base to prevent unauthorized persons.	2.76	0.79	Accepted
2.	Adding legal denials to outgoing mails.	2.80	0.46	Accepted
3.	Use of password for all confidential documents	2.61	0.79	Accepted
4.	Lucking down networks after office hours.	2.90	0.64	Accepted
5.	Use of firewalls.	2.85	0.64	Accepted

Source: Data 2022

From table III above, respondents accepted all the five(5) items on the technological related ways of preventing confidential information leakages. They were: adding legal denials to outgoing mails (X=2.76 SD=0.79); use of password for all confidential documents (X=2.80 SD=0.46); locking down of company official network after work (X=2.61 SD=0.79); use of firewalls to protect documents (X=2.90 SD=0.64) and encryption of files and data base (X=2.85 SD=0.64).

Discussion of Findings

The findings from this study revealed the ways of avoiding human related confidential information leakages in organizations which include paying ICT employees good salary, providing regular security for ICT staff, maintaining the use of one IT firm prohibit the use of USB among others. The finding is in consonance with the findings of www.quostar (2020), and Yousef (2019) Who asserted in their separate studies that human confidential information leakages could be avoided by organization implementing good salaries for IT staff, holding the firm or ICT staff accountable using paper shredder to destroy vital documents and even prohibiting the use of personal handsets in work place and the necessity of doing so if the organizations are to continue to remain in business. Also revealed were the technology related ways of avoiding confidential information leakages, which include encrypting files and data base, adding legal denials to outgoing mails, use of password for confidential documents and use of firewalls. This was corroborated by Greitzer, (2019) and Ritala et al (2016) who opined that organizations should encrypt their files and data base, add legal denials to outgoing mails, use password for confidential documents, use firewalls to amongst others in order to
achieve the sustainability of business.

Conclusions

Based on the data analysis, interpretation and findings, it was concluded that information such as employees information, customer's information, budget information etc are some of the types of confidential information leakages in the selected organizations. It was also concluded that confidential information leakages can be avoided through the combination of human and technology related ways such as encryption of firewalls, confidential files, use of password, paying ICT staff good salaries and allowances etc.

Recommendations

Based on findings and the conclusions drawn, it was recommended that the management of the selected organizations should as a matter of urgent necessity implement the following for the sustainability of their business.

1. All staff especially IT staff should be trained and retrained on regular bases on how to share company's confidential information of the organizations.
2. IT staff should be paid enhanced salaries and peculiar allowances to discourage them from trading company's confidential information.
3. Organization s should use one IT firm to control applications and softwares in the organizations.
4. All confidential information documents should be encrypted for safety reasons.
5. Management should also consider offsite record storage for additional security.
6. There should be penalty for those who leak confidential information of the organizations to serve as deterrent to others.
7. Use of password and firewalls should be adopted for confidential documents.

REFERENCES

Alneyadi, S., Elankayer, S., and Vallipuram, M. 2016. "A survey on data leakage prevention systems," *Journal of Network and Computer Applications* 6(2).

Greitzer, F. L, Purl J, Y. Leong M, sticha, P.J. (2019). "Positioning your organizations to respond to insider Treats," in IEEE Engineering Management Review, vol. 47 no 2 second quarter, Doi. 10.1109 EMR 2019. 2914612.

Mensah, J. (2019). Sustainable development' meaning, history, principles, pillars and implications for human actions interactions review. Cogent Social sciences: 5:1, 11535331 DOI 10 1080/23311886.

Morshed, U. C, Sutharsham, R, Biplob, R; Chowdhury R, S (2021). A Novel Insider Attack and Machine Learning Based Detection for Internet things. DOI.10.1145/3460721.

Pelteret, M. and Ophoff, J. (2016) https://www.researchgate.net/publication/312577391 A Review of information privacy and its importance to consumers and organizations.

Nzewanta,V.O. (2022), Avoiding Confidential Information leakage in Business Organizations in Minna Metropolis, HND Project, Department of Office Technology and Management, Federal Polytechnic, Bida, Niger State.

Ritala P. Clamder H, Michallova S. & Husted K (2016) Knowledge sharing, knowledge leaking and relative innovation performance. An empirical study Technovarion.(35) pp 23-31 *https://infowatch.com/node/2654/done?sid*=34.

Safianu, O. and Frimpong, T. (2016). Information system security threats and vulnerabilities: Evaluating the human factor in Data protection.international journal of Computer Applications. 143(5).DOI.10.5120/ijca2016910160.

Yousef Ahmed (2019) Protection and Defense against sensitive data leakage problem with organization.
https”//www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/2020.