INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN MULTIDISCIPLINARY STUDIES (IJARMS), VOL. 1, NO. 1, DECEMBER, 2021 ISSN 2756-4444
E-ISSN 2756-4452

INFORMATION SECURITY POLICY AND PRACTICES AMONG OFFICE MANAGERS IN TELECOMMUNICATIONS INDUSTRY IN NIGERIA

BY
Dr. Tolulope Elizabeth Adenekan: Department of Information Management, Lead City University, Ibadan; E-mail: tolu.adenekan@icu.edu.ng
&
Oluwatosin Abiodun Ologbosere: Department of Information Management, Lead City University, Ibadan; E-mail: oluwatosinologbosere@gmail.com

Abstract
The modern age is characterized by unprecedented information explosion and with the advent of globalization and ever-changing technologies the need for information security (IS) has become more vital. This motivate an enquiry into information security policy and practices in telecommunications industry. This study adopted a descriptive design with a sample of 30 employees randomly selected from Globacom telecommunication located in Oyo State. five research questions were raised and answered using frequency and simple percentage. The result showed that ISO framework was mostly adopted within telecommunication firm under study, information security and practices were generally low. The findings also reveal that larger percentage of employees from the telecommunication have little awareness of ISM practices. Among others it was recommended that every organization needs to apply security measures which controls systems and operations internally, and also protecting the integrity and data confidentiality. Telecommunication firms need to emphasize on ISM practices and policies as key factor that can enhance their competitive advantage. Timely, effective and sufficient training should to be undertaking by telecommunication firms in order to acquaint the various stakeholders such as employees, management staff on adoption, awareness, availability and effect of ISM practices and policies.
Keywords: Information, security practices, Telecommunication and Information policy

Introduction

Information is today regarded as one of the most valuable assets of an organization. With the advent of globalization and ever-changing technologies the need for information security (IS) is becoming more vital. Dependence on information, including for some of the world's largest organizations such as governments and multi-national corporations, has grown rapidly in recent years. However, reports of information security breaches and their associated consequences continue to indicate that attacks are still escalating on organizations when conducting these information-based activities. As organizations are becoming dependent on information technology the emphasis on IS is getting more significant. Information security relates to an array of actions designed to protect information and information systems. However, information security does not protect only the information, but also the whole infrastructure that makes its use easier. It covers hardware, software, and physical security. The more the number of applications, users and systems increase, the more the management of an organization's information security gets more complex and the vulnerability increases (May and Keller, 2017). Information security has been regularly considered to be a technological problem with a technological solution. Evidence suggest contrary opinion as information security have been shown to involves managing risks which consist of identifying and measuring threats to information assets in the organization and taking actions to address those threats (Jones,2007).

Information used in organization requires special protection for confidentiality, integrity and availability and, of course, some information used in organizations needs protection for more than one of these categories of information security. Such information might be sensitive employee or customer information, confidential business research or plans, financial information, or information falling under special information categories such as privacy information, health information, or certain types of financial information. Some of these information categories have special, much more restrictive regulatory requirements for specific types of information security protections. Failure to properly protect such information, based on the required protections, can easily result in significant fines and penalties from the regulatory agencies involved. Just as there is a cost involved in protecting information (for hardware, software, or management controls such as policies and procedures, etc), there is also a cost involved in not protecting information. However, the cost of not protecting information is far graver (Craig et al, 2015).

Furthermore, to have great security implementation, users or employees in organizations must comply with securing the information. Understanding the risks and prevention might help reducing the risk of security threats and data loss. Security is all about preventing all sorts of threats from the intentional and unwarranted actions. The objective

of information security management practices is thus to build protection against criminal actions intentionally. Telecommunications reach deep into the daily circumstances of individuals, businesses, and governments. Telecoms, in fact, touches nearly everything and everyone, and, along with energy, forms a foundation upon which all other critical infrastructure operates. A successful attack on a telecommunications operator could disrupt service for thousands of phone customers, sever internet service for millions of consumers, cripple businesses, and shut down government operations. The global fraud loss survey found that in 2016, the telecommunications industry suffered $38.1billion in fraudulent charges. The telecommunication industry is susceptible to attack because they hold large volumes of personal data, alliance and necessity to rely on global operative standards. It is worthy of note that telecommunication vulnerability exists on various levels such as hardware, software and human.

Furthermore, information security challenges in the global perspective has been traced to human incapability rather than technical issue, quite a number of researchers argued further that non-compliance with information security policy is one of the key challenges organizations are faced with and shortage of professionals (Shamsudin, 2019; Ben-David et all 2011). In Africa context Mutlaq et al (2016) asserted that information security is a combination of people, processes and technology however, information technology (IT) and office managers focused more on technology control. As high as attention is given to security, the IT systems are consistently under great attack which could be attributable to human error, unethical behaviour or unprofessionalism (Mohammad and Dorcas 2014). Hence, the need to institute information security management practices and policies in order to shield the organization from being vulnerable. The information security practices reduce or eliminate the risk of organization breeching information security policy which has a grave consequence for a member of organization to really practice or adhere to practices of information security to its optimal level.

Information security policies (ISP) is a set of procedures, rules put in place to ascertain that information technology users within an organization, establishments adhere to at least the information security and data/information protection. ISP supports appropriate behaviour among employees by ensuring the availability of clear instruction of responsibilities to follow as well the terms and conditions of the policy (Siponme et al, 2014). Information security policies are the primary concern of an organization's information security management, it is needed by organizations in order to protect the organization's critical information assets, explains what an employee should do and should not do as well as employees' reasonable behaviour in order to secure the information. Furthermore, Eisenberg, Lowe and Spitze (2014) states that an information security policy gives management direction and support for information security while Fisher, Erdelez and McKechine (2005) point out that the establishment of standards are a good starting point for creating the information security policy in order to enhance information security in organizations.

Lack of information security policy in organization puts the organization at risk. This means that the organization has a less understanding of its most sensitive data and information and does not have a strong awareness regarding possible exposures. Such gaps unfold the organization to cyberattacks and important security issues. With telecommunication industry extreme dependency on information technology (IT) the consequences of security breaches can be extremely grave (Bundy, 2002). In addition to monetary losses, breaches of information systems can also cause damages to businesses such as disruption of internal processes and communications, the loss of potential sales, loss of competitive advantage, and negative impacts on a company's reputation, goodwill and trust (Bruce, 2003). As a result, information security management practices and policies among the employees has become a required function (Abawajy, 2014). In many cases, it is impossible or nearly impossible to run a business without the smooth and secure operation of its information systems. Lack of awareness on the level of secrecy of document should be avoided by employee in avoiding unnecessary leakage. thus, protecting information has become less about technology and more about sustainability of the enterprise itself (National Institute of Standards and Technology NIST (2013). Clearly, more research is needed to better understand how organizations practices and adopt policy for information security.

Statement of the Problem

The paradigm shifts in the adoption and integration of information communication technologies (ICT) into businesses and organizations has witnessed unprecedented increase as companies strive to enhance their efficiency through adoption of ICT, albeit with its consequential security threat as large volume of information are received, shared and transferred as a result of ICT integration. Awareness of the possible threat to information required a conscious effort on the part of the telecommunication firms to deliberately orchestrate plans to protect the information. In protecting the information, it is expedient that information security should be a collective venture incorporating, person, process and technology. However, cursory observation reveals that information security has

too often been viewed in isolation, the perception being that security is someone else's responsibility and there is no collaborative effort to link the security program to business goals and employee's involvement. It is also evident that information security has not been rigorously pursued due to issues ranging from changing risk profile, funding, internal or external factors and cultural issues. this reveals the gap for an integrative approach to information security practices which not only focuses on technical measures but also the awareness of framework, policies and practices in order to ensure organizational and customers information are shielded from attack thereby increasing the standing of the organization. Thus, this study seeks to examine the security policy and practices among employees in Telecommunications Industry using Globacom Nigeria as a case study.

Objectives of the Study

The present study is guided with the following objectives:

1. Examine the information security practices management framework employed in the telecommunication industry.
2. Determine the level of awareness of ISM practices in the telecommunication industry.
3. Examine the Information Security Policy Practices in the telecommunication industry
4. Examine the level of availability of information security policies practices
5. Determine the level of effect of information security policies in the telecommunication.

Research Questions

1. What is the information security practices framework employed in the telecommunication industry?
2. What is the level of awareness of information security awareness of ISM practices in the telecommunication industry?
3. What is the Information Security Policy Practices in the telecommunication industry?
4. What is the level of availability of information security policies practices in the telecommunication?
5. What is the level of effect of information security policies in the telecommunication?

Methodology

The study adopted descriptive design; this method is advantageous for research due to its flexibility. The population consists of all 43 employees at the three branches (Secretariat, Challenge, and Sango) of Globalcom Telecommunication Company located in Ibadan metropolis. Total enumeration sampling technique was used. The main instruments of data collection were questionnaires. A total of 41 questionnaires were administered. The questionnaires consisted of closed and open questions, there are 25 questions with response format ran. The questions were divided into three sections. Section A contained general information about the organization, section B focused on ISM practices while section C focused on ISM practices awareness. Cronbach alpha of .76 was recorded when the questionnaire was pilot tested on respondents from airtel company who are not part of the main study. Data analysis was guided by the research objectives designed at the beginning of the research. The data was analyzed using descriptive analysis and Pearson Product Moment Correlation (PPMC).

Results

The study achieved a response rate of 80% Out of the 41 questionnaires seeking responses, 30 questionnaires were responded to.

Research Question 1: What are the information security practices framework employed in the telecommunication industry?

Table 1: Showing Participants Response Based on the Type of ISM framework Adopted

Framework	Frequency	Percent
COBIT	6	20.0
ISO	12	47.1
ITIL	3	10.0
None	9	30.0
Total	30	100

Table 1.1 reveals the type of ISM framework that telecommunication had adopted. majority (47.1%) indicated that ISO framework was mostly adopted within their organizations. This was followed by 30.0% who had not adopted any form of ISM framework. Similarly, 20.0% adopted COBIT, while 10.0% of the respondents indicated that the organization adopted ITIL. This implies that ISO framework is the mostly adopted by telecommunication firm.

Research Question 2: What are the level of awareness of information security awareness of ISM practices in the telecommunication industry?

Table 2: Showing Participants Response Based on the Awareness of ISM Practices.

Factors	Not aware	Slightly aware	Moderately aware	Well aware
Resource Management	5	15	7	4
	(17.0)	(50.0%)	(23.0%)	(13.0%)
Risk Management	10	5	3	7
	(33.0%)	(17.0%)	(10. %)	(23.0%)
Service Management	9	6	4	11
	(30.0%)	(20.0%)	(13.0)	(37.0%)
Strategic Alignment	13	7	5	5
	(43.0%)	(23.0%)	(17.0%)	(17.0%)
Business Alignment	15	8	2	6
	(50.0%)	(27.0%)	(7.0%)	(20.0%)
ISM Management	12	7	5	8
	(40.0%)	(23.0%)	(17.0%)	(27.0%)
ISM Policy	12	4	9	6
	(40.0%)	(13.0)	(30.0%)	(20.0%)

From the result presented in table 2, it is clear that the most employee in the sampled population lack awareness of ISM practices adoption. The percentage of 30% - 50.0% indicate that there is high percentage of lack of awareness in respect to ISM practices.

Research Question 3: What is the Information Security Policy Practices in the telecommunication industry?

Table 3: Showing Participants Response Based on the Information Security Practices

S/N	ITEMS	SA	A	D	SD	M	S.D
1.	Information security policy is an important policy for telecommunication	12 (40%)	12 (40%)	6 (20%)		3.2000	.70217
2.	There is need of an IS Policy to protect information.	3 (10%)	6 (20%)	9 (30%)	12 (40.0%)	3.3291	.71411

ISSN 2756-4444
E-ISSN 2756-4452

3.	It is very difficult to understand my organization's IS policy.	6 (20.0%)	15 (20%)	6 (20%)		2.8000	.88668
4.	It is very difficult to measure the level of satisfaction of my IS policy in my organization	6 (20.0 %)	18 (60.0%)	6 (20.0 %)		2.2000	.99655
5.	My organization monitors employees' hard copies documents	15 (50.0%)	6 (20.0%)	9 (30.0%)		2.7000	1.36836
6.	Employees are informed before monitoring their computer activities.	3 (10.0%)	24 (80%)	3 (10.0%)		3.0000	.45486
7.	Employees have the right to use their office e-mail for personal e-mail as well.	6 (20.0 %)	15 (50.0%)	8 (2.6%)		2.8000	.88668
8.	My organization scan employees' emails before it reaches relevant email box.	6 (20.0%)	3 (10.0%)	6 (20.0 %)	15 (50.0%)	2.0000	1.20344
	Weighted Mean	**2.81**					

Table 3 above indicate the response of the respondents to ISM practices in the telecommunication industry, the table reveals the weighted mean of 2.81 out of the 4.00 maximum obtainable score, which is higher than the standard mean of 2.50. this implies that respondents are aware of information security practices. Out of the 8 items used to measure awareness of ISM practices in the telecommunication, only three items were above the weighted mean score and this contribute to the awareness of ISM practices. The three items are **:** There is need of an IS Policy to protect information (3.33>2.81) is ranked the highest among the mean score rating, followed by Information security policy is an important policy for telecommunication(3.2000>2.81), and employees are informed before monitoring their computer activities (3.000>2.81). while the remaining five items with mean score less than weighted mean are not contributing to awareness and ISM practices. This implies that majority of the respondents are inadequately aware of ISM practices in the telecommunication industry.

Research Question 4: What is the level of availability of information security policies practices in the telecommunication?

Table 4: Showing Participants Response Based on the Availability of ISM Policies in Telecommunication Industry.

S/N	Items	SA	A	D	SD	M	S. D
1	Employees are given chance	3	24	3		2.0000	.81368

	to have a better understanding of IS policy through company intranet.	(10.0 %)	(80.0%)	(10%)			
2	Employees are given a chance to have better understanding of IS policy through company library.		18 (60%)	6 (20.0%)	6 (20.0%)	2.5000	.82001
3	Contents of IS policy are not properly communicated to the employees via superiors.	21 (70.0%)	3 (10.0 %)	6 (20.0%)		2.3000	.91539
4	Changes done to IS policy are properly circulated to all the employees.	18 (60.0%)	3 (10.0%)	9 (30.0%)		2.1000	1.06188
5	Employees are not given an opportunity to have a complete understanding of IS policy at the joining.	3 (10.0%)	9 (30.0 %)	6 (20.0%)	12 (40.0%)	2.2000	1.18613
Weighted Mean		**2.22**					

Table 4 reveals the responses of telecommunication workers on the availability of information security policy. The weighted mean of 2.22 out of the 4.00 maximum obtainable score which is lower than the standard mean of 2.50. Only two items; employees are given a chance to have better understanding of IS policy is greater than standard score (2.500 >2.22) and contents of IS policy are not properly communicated to the employees via superiors (2.300 >2.22). Other items are below the weighted mean, an indication that information security policies is sparingly available in the telecommunication industry.

Research Question 5: What is the level of effect of information security policies in the telecommunication?

Table 5: Showing Participants Response Based on the Enforcement of ISM Policies

S/N	**Items**	**SA**	**A**	**D**	**SD**	**M**	**S.D**
1	My organizations policy has not been properly enforced.	6 (20.0%)	6 (20.0 %)	6 (20.0%)	12 (40.0 %)	2.2667	.90719
2	There are loop holes in my organizations IS policy	5 (16.7%)	2 (6.7%)	19 (63.3%)	4 (13.3%)	2.6000	.96847
3	Most of the employees are not satisfied with our IS policy and how it was enforced	7 (23.3%)	7 (23.3 %)	13 (43.3%)	3 (10.0%)	3.4856	.52558
4	In my organization, employees are strictly monitored for IS Policy violations	9 (30.0%)	6 (20.0%)	15 (50.0%)		3.1885	6.32655

ISSN 2756-4444
E-ISSN 2756-4452

5	In my organization, IS Policy violators are penalized at first place without giving any chances	5 (16.7%)	2 (6.7%)	19 (63.3%)	4 (13.3%)	3.2173	.62334
6	In my organization, violating IS policy may lead to employee termination	6 (20.0 %)	15 (50.0%)	8 (2.6%)	6 (20.0 %)	3.1757	.74536
Weighted Mean		3.12					

Table 5 indicates the response of respondents in respect to enforcement of information security policy. The table reveal weighted mean score of 3.12 out of the maximum 4.00 maximum obtainable. The weighted mean is greater than the standard mean. of the six items, four items were above the weighted mean. these are : Most of the employees are not satisfied with our IS policy and how it was enforced (3.48> 3.12), In my organization, IS Policy violators are penalized at first place without giving any chances (3.21> 3.12), In my organization, employees are strictly monitored for IS Policy violations (3.21> 3.12), In my organization, violating IS policy may lead to employee termination (3.21> 3.17). while two items; my organizations policy has not been properly enforced (3.21>2.26) and there are loop holes in my organizations IS policy 3.21>2.26000). this implies that enforcement of information policy is high.

Discussion

The first research question examined the information security practices framework employed in the telecommunication industry. The findings indicated that ISO framework was mostly adopted. This finding is in line with the work of Madiavale (2014) who reported ISO is the most frequently adopted model at the expense of other available models. This present an evidence that telecommunication companies are yet to adopt broader framework that incorporates most aspect of the organization in respect to ISM.

The second research question asks; what are the level of awareness of information security of ISM practices in the telecommunication industry. The result emanating from the study reveals that most employees are not aware of ISM practices adoption. This finding converges with the work of Fayez (2017) who found that employees at telecommunication companies are not adequately aware of ISM practices governing their affairs. The framework put in place to control and manage information risks is referred to as information security management. The adoption of ISM and its practices propels organizations to achieve organizational and business goals which enhances competitive advantage. The findings of the study present an evidence that telecommunication companies have not done adequately adopt ISM practices or are yet to adopt broader framework that incorporates most aspect of organization in respect to ISM. This finding is corroborated by the work of Moneer, Sean, Atif and Shanton(2015) which emphasize in terms of awareness of ISM practices. It is evident from the findings that a larger percentage of employees from the telecommunication have little awareness of ISM practices.

The third research question bothers on the Information Security Policy Practices in the telecommunication industry. The findings reveal that majority of the respondents are inadequately aware of ISM practices in the telecommunication industry. The finding is in tandem with the work of Nader, Rossouw & Steven (2016) who reported that even those that have adopted any ISM framework, there is inadequate in-depth analysis of these practices. This thus creates a gap between understanding ISM practices and adopting them.

The fourth research question examined the level of availability of information security policies practices in the telecommunication. The result shows that information security policies are sparingly available in the telecommunication industry. The finding is supported by Seapei & Salah (2019). Those organizations that have adopted framework and ISM practices lacks policies to guide its adoption and execution.

The fifth research question examined the level of information security policies in the telecommunication industry. The result indicated that the effect of enforcement of information policy would be very high on telecommunication industry provided its well adopted. This finding is in convergence with Madaivale (2014) report that organizations need to ensure more awareness of information security management. Awareness of information security management can be achieved through establishment of information security policies that are backed by global

standard. The comprehensive ISM program that is capable of integrating organization, stakeholders, processes and technologies interaction and how organizations decision makers, human factor and other key elements in the organization can curb threat against information and manage risks associated with daily accumulating information.

Conclusion

Information in various forms is the most important asset for most organizations and especially telecommunication. It is crucial that telecommunication industry work systematically and need to secure the information so that it is confidential, accurate and accessible. To achieve this, appropriate and all-encompassing ISM framework need to be adopted and more efforts needs to be geared toward creating awareness about the ISM policies and practices.

Recommendations

It is recommended that:

1. Every organization needs to apply security measures in which controls systems and operations internally, and also protecting the integrity and data confidentiality.
2. Telecommunication firms need to emphasize on ISM practices and policies as key factor that can enhance their competitive advantage.
3. Timely, effective and sufficient training needs to be undertaking by telecommunication firms in order to acquaint their various stakeholders such as employees, management staff on adoption, awareness, availability and effect of ISM practices and policies.
4. More need to be done by regulatory agencies in term of attaching importance to ISM as well as increase the allocation towards the development and sustainability of ISM in telecommunication firms.

References

Abawajy, J. (2014). User preference of Cyber Security awareness delivery methods. *Journal Information Technology* DOI:10.1080/0144929X.2012.708787

Antoni, C & Gustavo, P. (2015). Measuring user satisfaction with information security practices *Journal of Computer & Security vol 48, 267-280*

Ben-David Y, Hassan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., and Brewer, E.A. (2011). Computing security in the developing world: A case for multidisciplinary research. In proceedings of the 5th ACM workshop on Networked systems for developing regions.

Bruce, B. C. (2003). Literacy in the information age: inquiries into meaning making with new technologies. Newark: International Reading Association.

Burbules, N. C. and Callister, Jr, T. A. (2000). Watch IT: The risks and promises of information technologies for education. Illionois: Westview Press.

Bundy, A. (2002). Growing The community of the informed: information literacy a global issue. Australian academic and research libraries, 33 (3): 125-134.

Craig, A., Horne, A., Ahmad, S. and Maynard, B. (2015). Information Security Strategy in Organisations: Review, Discussion and Future Research Directions. Australasian Conference on Information Systems.

Eisenberg, M. B., Lowe, C. A. and Spitzer, K. L. (2014). Information literacy. Westport: Greenwood Publishing Group.

Fisher, K. E., Erdelez, S. and McKechnie, L. (2005). Theories of information behaviour. Medford: Information Today.

Fayez H. (2017) Developing an Information Security Policy: A Case Study Approach: 4th Information Systems International Conference, Published by Elsevier.

Jones, A. (2007). A framework for the management of information security risks. BT Technology Journal, 25(1), 30-36.

Ludwig, S & Parvis, P. (2014). Students Information Security Practices and Awareness. *Journal of Information Privacy and Security* 8:4, 3-26 doi: 10.1080/15536548.2012.10845664.

Madiavale, B. A. (2014). Information Security Management Practices And Organizational Goals: A Study Of Microfinanace Organizations In Nairobi.

May, W and Christina, K. (2017). Implementation of information security policies in public organizations: Top management as a success factor ile:///C:/Users/%60hp/Desktop/information%20security%20paper/FULLTEXT01.pdf

Mohamad, H. & Dorcas, A. (2014). Mediating effect of information security culture on the relationship between information security activities and organizational performance in the Nigerian banking setting: *International journal of Business and Management* vol 9, No 7. ISSN 1833-3850.

Moneer, A., Sean, B., Atif, A., and Shanton, C. (2015). Information security policy: A management practice perspective. *Journal of Information Policy Management Practices*, Australasian Conference on Information Systems.

Mutlaq A., Steven, F and Nathan, N. (2016). Information security policies: A review of challenges and influencing factors. Conference paper DOI: 10.1109/ICITST.2016.7856729.

Nader, S., Rossouw, V. & Steven, F.(2016). Information Security Policy Compliance Model in Organisations. *Journal of Computer& Security* vol 56 (1-13) 2016.

Seapei, N. & Salah, K (2019). Challenges in Information and Cyber security program offering at higher Education Institutions, proceedings of 4th international conference on the internet, cyber security and information systems.

Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information Security Behaviours among Employees. *International Journal of Academic Research in Business and Social Sciences*, 9(6), 560–571.

Siponeme, M., Mahmood, M., and Pahnila, S. (2014). Employees' adherence to information security policies: *Journal of Information and Management*, 51:217-224.