Computing, Information Systems & Development Informatics Journal

Volume 3. No. 2. May, 2012

Employee's Conformity to Information Security Policies- The Case of a Nigerian Business Organizations

ADEDARA, Olusola
Department of Computer Science
The Federal Polytechnic
Ado-Ekiti
Nigeria
fafvfk@yahoo.com

KARATU, Musa Tanimu
Computer Department
Faculty of Science
University of Ibadan
Nigeria

OLAGUNJU, Abiodun
Department of Computer Science
University of Ibadan
Ibadan, Nigeria
abbeylag@yahoo.com

Reference Format: Adedara, O., Karatu, M.T. & Lagunju, A. (2012). Employee's Conformity to Information Security Policies In Nigerian Business Organisations (The Case of Data Engineering Services PLC). Computing,, Information Systems & Development Informatics Journal. Vol 3, No.2. pp 43-50

Employee's Conformity to Information Security Policies – The Case of a Nigerian Business Organizations

Adedara, O.; Karatu, M.T. & Lagunju, A.

ABSTRACT
We evaluated employee's conformity to information security policies using four research questions and three research hypotheses. A survey research methodology was used to evaluate staff of the case study (Skannet) using both questionnaires and interview. Data gathered were analysed using both descriptive and inferential statistics. The findings of this study reveal that majority of Skannet's employees have adequate knowledge of Skannet's information security policies. However, the level of employees' compliance with the ICT policies is very low. Among organizational measures put in place by Skannet to ensure information security compliance include regular training / re-training for staffs on policies, regular survey sent to all staff to test level of awareness and punitive measures by Human Resource Department. The study further revealed that Skannet's Information Security policy positively affect the attainment of organizational goals such as improvement in quality of services, promotion of information sharing, transparency and accountability among staffs in the organization
.

Keywords*:* Policies, security, compliance, training and services.

1. INTRODUCTION

The Internet is a collection of networks linked together using a common protocol – global computer network achieved through the interconnection of smaller computer networks around the world. People, computers and information are link together electronically by a common protocol or set of communication rules. It should be evident now why telecommunications, broadcastings and the internet all have to be dealt with not necessarily by a single policy but within a single policy frame work. They all use the same infrastructure to transmit messages (copper cable, optical fiber, satellites) over the radio spectrum and they can all deliver the same content (voice, data text, pictures, videos etc) to the same users. (Kate Wild 2004).

Information Security policies generally covers three areas, they are:

1. Telecommunication
2. Broadcasting
3. Internet (Networking Technologies)

A corporate policy is usually a documented set of broad guidelines formulated after an analysis of all internal and external factors that affect the firms objectives, operations and plan, formulated by the firm's board of directors. (Folayan, 2010, Boubakar, 2008). Information security on the other hand is the process of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the information stored is highly confidential and not for public viewing. (Toni & Tsubuira, 2002).

Effective information security systems incorporate a range of policies, security products, technologies and procedures. Software applications which provide firewall information security and virus scanners are not enough on their own to protect information. A set of procedures and systems needs to be applied to effectively deter access to information. (Steve, 2008; ISP US, 2004)

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. (Wikipedia 2011).

1.1 Knowledge Gaps

Information and communication technology is increasingly penetrating all social and economic activities. It is a high stake game that involves all sectors of society comprising many stakeholders. Information Security policies are often made as a result for concern for issues bothering on system vulnerabilities occasioned by authorized usage. Information Security policy is a set of principles or a broad course of action that guides the behavior of governments, organizations, corporations and individuals (Steve, 2008). Information Security policy covers information and communication technologies network, services, markets and relationships between the different actors involved in these – from the operators of submarine cable systems to the users of telecentres (Microsoft, 2010; OECD, 2012).

It may be national or international in scope. Each level may have its own decision making bodies, sometimes taking different or even contradictory decisions about how Information Security will develop within the same territory (David, 2009). In order to give staff members the feelings of autonomy and a sense of belonging, they need to know the rules and allowable usage limits of organization al information systems. These go beyond what time to show up, vacation time and health benefits. Written company policy that covers Information Security policy must be produced and adhered to.

This paper identifies and evaluate the manner in which Information Technology policies are defined and the level of usage compliance in a corporate setting using General Data Engineering Services (Skannet) Nigeria as a case study. The paper attempts to ascertain Skannet's Information Security policies awareness by the employees; examine the extent to which the employees comply with the Information Security polices; identify organizational measures instituted by Skannet to ensure policy compliance by employees; ascertain the impacts of Information Security policies on Skannet's organizational goals and make recommendations on Skannet's Information Security policies improvement.

2. EXISTING INFORMATION SECURITY POLICY AT SKANNET

General Data Engineering Services being an Internet Service Providing Company has certain rules and procedures governing what users can do on her network (Folayan, 2010). This Information Security Policy is as highlighted below.

Access Management and Control
To prevent or minimize unauthorized access to computer systems or damage, theft or loss of equipment, the following must be adhered to:

1. Physical Control

a. Access to server room and other major ICT facilities should be adequately secured at the doors and windows and only authorized persons can be allowed into the Server room.
b. The Contact Centre is required to maintain a Register (access log) where authorized staff logs in any activities carried out in the server room.

Logical Control

a. Each user (staff and client) on the network must have a Username and Password to access networked facilities.
b. Both staff and client username must not exceed eight characters. The password can be as long as desired by the users.
c. Each staff upon appointment must fill a staff account creation form. The form shall be administered by the human resource department.
d. The newly appointed staff will submit the completed form which must be signed by his supervisor to the officer on duty at the contact centre.
e. The duty officer is responsible for creating new staff accounts and activating the account on the network.
f. The duty officer should ensure that the entries in the form is correctly filled and signed by the staff before creating such account.
g. Each prospect/client will fill an account creation form at sign-up.
h. The client sign-up form will be administered by the Marketing Department.
i. The contact centre shall activate such account upon verification of the client identity.

Internet Usage

It is unacceptable to use General Data Engineering Services networks to:

a. View, make, publish or post images, text or materials that are, or might be considered as illegal, paedophilic or defamatory.
b. View, make, publish or post images, text or materials that are, or might be considered as, indecent, obscene, pornographic or of a terrorist nature.
c. View, make, publish or post images, text or materials that are or might be considered as, discriminatory, offensive, abusive, racist or sexist when the context is a personal attack or might be considered as harassment.
d. Send Spams, unwanted and unsolicited emails.

Network Control

a. The setup of PCs, laptops, printers, etc for network access should be done by the Engineering Department (GDES Workshop).
b. Point-to Point-over-Ethernet should be setup for the user's authentication on the network during the installation.
c. The company antivirus should be installed on each staff Computer. The License shall be administered by the Engineering Department.

Others include Troubleshooting, Repairs, Maintenance and Replacements; Disaster Recovery and Contingencies and Electronic Mail (Email),

3. RESEARCH METHODOLOGY

In this study, research design using a descriptive method was used, the population of design and the population of study. Sample size and sampling technique was used to manage the research work. Data collection procedure such as questionnaires, personal interviews, was instruments used for collection of data. Data analysis method used were descriptive statistical method of sample frequency counts and percentages were used to analyze the demography and research questions while inferential statistics of T-test, ANOVA and Chi-square was used to analyze the hypotheses.

3.1 Research Questions

Based on the foregoing, the research questions that this paper seeks to address include:

a. What is skannet's employees' awareness level of Information Security policies?
b. To what extent do Skannet's employees comply with Information Security policies?
c. What are the organizational measures put in place by Skannet to ensure Information Security policies compliance by employees?
d. What are the impacts of Information Security policies on Skannet's organizational goal?

3.2 Research Hypothesis:

Hypothesis 1: There will be no significant difference between Skannet's employees compliance with Information Security and attainment of organizational goals.

Hypothesis 2: There will be no significant relationship between Skannet's employees department and employees' policy compliance

Hypothesis 3: There will be no significant difference between Skannet's employees Information Security policies awareness and compliance.

3.3 Research Design

The research design adopted for this study was survey descriptive research method. This method was adopted because it enabled the researcher to collect data on the concerns of this study from the population at the locations of the population and to describe in a systematic manner the state or condition of the objects of research in this study.

3.3.1 Population Of The Study

The population of this study is made up of this staff and management of General Data Engineering Services in the South-western Zone and East of Nigeria; this include Oyo, Ogun, Kwara, Ekiti and Enugu State. A total number of ninety-six Skannet staff is in these states.

3.3.2 Sample Size And Sampling Technique

The entire population of this study, a census, was used in this study because it was manageable by the researchers.

3.3.3 Research Instruments

A self-designed questionnaire was used to collect data from this study. The instrument was divided into two sections A and B. In section A, the demography of the respondents such as age, years of experience, sex, marital status, educational background and religion was solicited. In section B, questions meant to solicit information to answer all research questions and hypothesis were asked. The instrument contained both open-ended and close end questions. Also, an interview guide was used to interview six Heads of Departments at Skannet.

3.3.4 Validation Of Instrument

In order to ensure both face and content validity of the instrument, the questionnaire was submitted to the researcher's supervisor and two other scholars for constructive criticisms. It was after their corrections were effected that the researcher went to the field to administer questionnaire.

3.3.5 Data Collection Procedure

The researcher distributed copies of the questionnaire among the staff of Skannet in the South-Western Zone division of the organization. Along with two other research assistants, the researcher made sure that the respondent were given adequate time to fill the questionnaire and to ensure high return rate, the instrument was handed over to solicit the assistance of the authority figures in the offices.

Data Analysis Method

Descriptive statistical methods of simple frequency counts and percentages were used to analyse the demography and research questions while inferential statistics of T-test, ANOVA and Chi-square was used to analyze the hypotheses.

4. DATA PRESENTATION AND ANALYSIS

This section is divided into two; section A is on the demography and section B presents data to validate the hypothesis raised in the study. The data are first presented in tables before they are presented in essay form; inferences are made from the data.

SECTION A

Table 1: Distribution of Respondents By Departments

Departments	Frequency	Percentage (%)
I.T	13	14.8
Customer Care	7	8
Sales	8	9.1
Finance	3	3.4
Transmission	3	3.4
Transmission Planning	8	9.1
Switch	3	3.4
Site Acquisition	8	9.1
Site Maintenance	6	6.8
Radio Frequency	7	8
HR	13	14.8
Fleet Management	6	6.8
Total	88	100

The above table shows various departments at General Data Engineering Services. The organisation has twelve (12) departments. It is evident from the data that 13 (14.8%) respondents are from Information Technology department, 7 (8%) respondents are from Customer Care, 8 (9.1%) are from Sales department, 3 (3.4%) respondents are from Finance departments, 6 (6.8%) respondents are from Transmission, 8 (9.1%) respondents are from Transmission Planning department, 3 (3.4%) respondents are from Switch department, 8 (9.1%) respondents are from Site Acquisition department, 6 (6.8%) respondents are fro Site Maintenance department, 7 (8%) respondents are from Radio Frequency Department, 13 (14.8%) respondent are from HR department while 6 (6.8%) respondents are from Fleet Management. The data implies that the respondents cut across all departments in the organization; they will make their contributions in this study to be perspectives.

SECTION B

Research Question 1:

What are the employees' awareness levels of Skannet's Information Security policies?

Organizational employees are to know about policies before such could be obeyed. This research question is to ascertain employee's awareness of Information Security policies.

Table 2: Skannet's Employee Awareness of Information Security policies

Question	Options	Frequency	(%)
Is there any policy on Information Security at Skannet?	Yes	71	80.7
	No	17	19.3
	Total	88	100

Table 2 shows the data on Skannet's employees Information Security awareness. It is obvious from the data that majority of the respondents are 71 (80.7%) affirm that there are policies on Information Security at Skannet while 17 (19.3%) respondents decline. These data is an indication that many of the employees are aware or rather they know about the policies guiding the use of Information Security at Skannet. It could therefore be inferred that Skannet Management does intimate the employee with the policies. However, these data do not indicate the degree of the employees' awareness. Therefore the next question is asked and answered.

Table 3: Degree of Information Security Awareness By Skannet Employees

Question	Options	Freq	(%)
How much of the Information Security Policy do you know?	Much	54	61.4
	Very Much	21	23.9
	Not Much	3	3.4
	Not Very Much	10	11.4
	Total	88	100

In Table 3 data on the degree of Skannet's employees Information Security awareness is revealed. It is evident in the data that 54 (61.4%) respondents know "much" of the policy, 21 (23.9%) respondents know "very much" of the policies, 3(3.4%) respondents know "not much" of the policies while 10 (11.4%) respondents know "not very much" of the policies. The employees generally speaking are expected to know details of the Information Security policies because of its importance to daily operation or organisational conduct of the workers. Meanwhile as it could be logically expected, the data reveals that vast majority of the workers are familiar with the details of Information Security policies at Skannet.

Meanwhile, interviews conducted for six departmental heads reveals that Information Security policy orientation which acquaints employees with specific details of how Information Security policies are to be applied is a usual orientation course for all staffs that are deployed to the departments. According to some of these interviews, because Skannet's operations are Information Security based, it is of utmost necessity for the staff to be oriented on how to and how not to use the Information Security

Research Question 2:
To what extent do Skannet employees comply with Information Security policies?

Table 4. Employees Compliance with Information Security

Question	Options	Freq	(%)
Do you comply with policies on Information Security	Yes	61	69.3
	No	27	30.7
	Total	88	100

Table 4. reveals that majority of Skannet's staff do comply with Information Security policies of Skannet. In the table, 61 (69.3%) respondents affirm that they do comply while 27 (30.7%) respondents claim that they do not. The data indicates that worker's compliance with the Information Security policies at Skannet is not doubtful. This implies that the staffs are not only aware of the policies but they do also comply.

Meanwhile five out of seven head of units interviewed submit that the level of workers compliance with the Information Security policies is low. For example, some of them affirm that the staff secretly and sometimes openly flout the policies when they know that they are not being monitored or supervised. At a point, one of them points out that staffs are not mindful of the policies at all until a re-orientation programme was organized in 2010.

Table 5: Extent to which Skannet's Employees Comply with Information Security Policies

Question	Options	Freq	(%)
To what extent do you comply with Information Security policies?	Great Extent	10	11.4
	Some Extent	21	23.9
	Little Extent	51	57.9
	No Extent	6	6.8
	Total	88	100

Table 5 shows that 31 (35.3%) respondents do comply with the Information Security policies to a large extent while 57 (64.7%) respondent do comply to little/no extent.

The above finding is an indication that most staffs at Skannet do comply with the Information Security policy to a small extent. Therefore, there appears to be a gap between the knowledge of the policies and the compliance with the same. In essence, there is apparent disregard for the policy. These findings substantiate the submission unit heads earlier presented which indicated that Skannet staffs give little regards to Information Security policy implementation.

Research Question 3:
What are the organizational measures put in place by Skannet to ensure policy compliance by employees? It is an organizational practice to put measures that will ensure compliance to corporate policy in place. Therefore, this question is to identify the corporate measures put in place by Skannet to ensure Information Security policy compliance.

Table 6: Organizational Measures Put in Place by Skannet to Ensure Information Security Policy Compliance

Measures	Frequency	(%)
Regular Communication from management to staff on Information Security policies	82	93.2
Regular training/re-training of staffs on policies	61	69.3
Regular surveys sent to all staffs to test level of awareness	68	77.3
Compulsory tests taken on Information Security by staffs	71	80.7
Punitive measures by Human Resources Department	68	77.3

Table 6 shows data on organizational measures put in place to ensure that staffs comply with the Information Security policies. It is evident from the table that 82 (93.2%) respondents acknowledge that regular communication from the management to the staffs on policies is to ensure that policies are adhered to, 61 (69.3%) respondents affirm that a regular training and retraining is another measure, 68 (77.3%) respondents affirm that a regular survey is usually sent out to test level of staffs awareness to Information Security policies; also, 71 (80.7%) respondents affirm that compulsory tests are taken by staffs on Information Security policies; the last item on the table reveals that Punitive measures are used by Human Resources Department to ensure compliance with Information Security policies.

Research Question 4:
Table 7: What are the impacts on Information Security policy on the attainment of Skannet's organizational goal?

Question	Options	Frequency	(%)
Do you think Information Security policy of Skannet positively affect attainment of organisational goals	Yes	69	78.4
	No	19	21.6
	Total	88	100

In Table 7, majority of the respondents 69 (78.4%) respondents affirm that Information Security policy positively affect the attainment of Skannet's organizational goal. Human Relation head of Skannet, when interviewed affirmed in consonance with the findings of the staff respondents.

According to him, policies are put in place because both the organization and its workforce will be beneficiaries; therefore, it is self-evident that the policies are there to take care of the work effectiveness in the organization.

Table 8: Impacts of Information Security policy on Skannet's Organizational Goals

Impacts	Frequency	(%)
It improves quality of service and products in the organization	59	67
It promotes information sharing, transparency and accountability among staffs in the organization	56	63.6
It provides information and communication facilities and services at reasonable costs	62	70.5
It provides individuals and organization with adequate Information Security knowledge	71	80.7

In table 8, 59(67%) respondents affirm that Information Security policy of Skannet improves quality of services and products in the organization, 56(63.3%) respondents affirm that it promotes information sharing, transparency and accountability among staffs in the organization; it also provides information and communication facilities and services at reasonable costs and lastly, it provides individuals and organizations with adequate Information Security knowledge.

The findings in the above data reveal that the policies on Information Security in Skannet have impacts on attainment of to ensure compliance with Information Security policy (Ibrahim, 2010; Davis, 2008.

The findings in the above data reveal that there are organizational measures in place at Skannet's to ensure implementation of Information Security policies. Among measures put in place are regular Information Security policies and preventive measures. Customer care unit head, sales unit head and Human relations, rear to corroborate the findings of the questionnaire; According to the trio, the attention of Skannet is focused on awareness of Information Security policy. According to them when revile round and are frequently reminded they would do, this is the organizational belief of Skannet. However, as it has been earlier established in this study that through there is awareness of the policy but the policy adherence by staff is low, according to one of the interviews the reason behind this is because Skannet as an organization care less about adherence because, according to him, he has never seen anybody punished for flouting the policy.

Hypothesis 1: There will be no significant difference between Skannet's employee's compliance with Information Security and attainment of organizational goals.

ANOVA test is used to test the above hypothesis. The data is represented below:

Table 9: ANOVA test on Skannet's employee's Information Security policies Attainment of Organizational Goal.

F	t	Df	Mean Difference	Std. Error Difference	Sig (2-tailed)	Decision
627.291	10.067 -6.648	86	-6296 -6296	0.6254 0.09471	0.000	*Sig

The above table reveals that the test result .000 is less than 0.05 level of significance (P.000<0.05 alpha level). This result is an indication that there is a significant difference between the variables tested. Therefore, it is established that there is a significant difference in Skannet's employees' compliance with Information Security and attainment of organizational goals.

Hypothesis 2: There will be no significant relationship between Skannet's employees department and employees' policies compliance.

A Chi-square test is used to test the above hypothesis and the result is represented in Table 10. :

Table: Chi-square test on Skannet's Employees Department and Employees Information Security Policy Compliance. Cross tabulation On Employees Department and Compliance with Information Security. The chi-square test reveals that the result is .000 which is less than 0.05 level of significance (p.000<0.05 alpha level).

This result is an indication that there is a significance difference between the variables tested. It is therefore evident that there is a significant relationship between Skannet's employees departments and employees' policies compliance. The hypothesis is therefore rejected. In essence, there is a significant relationship between Skannet's employees departments and employees' policies compliance. This finding is an indication that Skannet's employees department determines employees' compliance with Information Security policies. This finding is understandable when the fact that some departments are more prone to use Information Security in the organization than the other(s).

Hypothesis 3: There will be no significant difference between Skannet's employees Information Security policies awareness and compliance.
A test is used to test the above hypothesis and the data are presented below;

Table 10: A T-test on Skannet's employees Information Security policies awareness and compliance.

F	t	Df	Mean Difference	Sig (2-tailed)	Decision
827.291	-10.067 -6.648	86	-.6296 -.6296	.000	*Sig

The above table reveals that the t-test result is .000 which is less than 0.05 level of significance (p.000<0.05 alpha level). This result is an indication that there is a significant difference between the variables tested. The hypothesis is rejected. It is therefore evident in this study that there is a significant difference between Skannet's employees Information Security policies awareness and compliance. This is an indication that Skannet's employees' awareness of information security policies does not translate into compliance of information security policies

5. CONCLUDING REMARKS

A policy is a deliberate plan of action to guide decision and to achieve organizational goals. Though it (policy) has lofty roles in any organization, it is doubtful if employees pay strict adherence to it, especially Information Security policies. In Skannet, the observation reveals a likelihood of employees flouting Information Security policies. Our study appraised the impact of Information Security policies on attainment of organizational goals.

Findings from data gathered revealed that Skannet's Information Security policy positively affects attainment of organizational goals; among impacts of the Information Security policy includes improvement in the quality of services and products in the organization; promotion of information sharing, transparency and accountability among staff in the organization, provision of information and communication facilities and services at reasonable cost and provision of individuals and organization with adequate Information Security knowledge.

Employees compliance with the Information Security policy in the case study significantly affect attainment of Skannet's organizational goals. Also, the department of the employees, it is revealed, determines employee compliance with Information Security policies and lastly, it is discovered that employees awareness of Information Security policies does not translate to compliance with the same policy.

Attainment of organizational goals is always a paramount issue in the heart of the corporate body managers. To ensure this attainment, policies are instituted by organizations to guide the conducts of the workforce. This practice, it is found out in this study, is not an exception at Skannet. However though it is revealed in the study that Information Security policies do influence attainment of Skannet's organizational goals, it appears that little attention is paid to its implementation or adherence by both management and the workforce.

REFERENCES

Boubakar, B (2008). ICT Policy; Development Workshop Kigali Kenya. www2.aau.org/ledev/new_ledev2_report.pdf

David, C. (2009). Out of the Shadows: Preventive Detention, Suspected Terrorists, and War. Carlifornian Law Review. scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1370...

David, S. (2008). Association of Progressive Communication ICT Policy handbook. www.apc.org/en/system/files/APCHandbookWeb_EN.pdf

Folayan, S. (2010). Security Policy Handbook General Data Engineering Services PLC (GDES),www.skannet.com

ISP US (2004). Policy on Information Security Program US Department of Health and Human Service, HHS IRM Policy 2004-002.001 Published on 15th of Dec 2004 . www.hhs.gov › OCIO Home

Ibrahim, H. (2010). Kenya Teachers Service Commission ICT Policy. www.tsc.go.ke/downloads/Policies/ict.pdf

ISP US (2004). Policy on Human Services, on Rules of Behavior. www.hhs.gov › OCIO Home

Kate, W (2012). Handout for Multimedia Training on ICT Policy. www.apc.org/english/capacity/.../mmtk_ictpol_intro_handout.doc

Microsoft ISP (2010). Information Security Policy for Microsoft Trustworthy Computing USA. http://www.microsoft.com/twc

OECD (2002). OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security were adopted as a Recommendation of the OECD Council at its 1037th Session on 25 July 2002. http://www.oecd.org

Steve, T. (2008). Information Security Handbook from University of Auckland. www.cs.auckland.ac.nz/~cthombor/

Toni, B. & Tusubira F.F (2002). How to Roll Out an ICT Policy in Your Organization. www.techrepublic.com/...roll-out...policy-in-your-organization/1051.

Wikipedia (2012) . ICT Policy. http://en.wikipedia.org/wiki/access-control