Determinants of Information Security Awareness among Employees of Capital Market Registrars in Lagos, Nigeria: An Empirical Study

Samuel Oluranti Oladipupo
Africa Regional Centre for Information Science (ARCIS), Ibadan, Nigeria
E-Mail: samladoluy2k5@yahoo.co.uk

Abstract - **The purpose of the study is to examine the determinants of information security awareness (ISA) among employees of Capital Market Registrars (CMRs) in Lagos, Nigeria based on established factors from the existing literatures on ISA. The main objectives of the study are; to determine the level of information security awareness among CMRs' employees and to identify the components that influence information security awareness. This study utilised a survey design. Stratified random sampling technique was used to select the respondents for the study. A total of 326 copies of questionnaires were distributed among the employees in CMRs, of which 267 properly completed questionnaires were returned. Descriptive statistics and simple regression were used for data analysis. Finding revealed that information security policy, information security education, knowledge of technology, and employee's behaviour significantly influenced information security awareness. The results of the study further revealed the strong correlation between employee's behaviour and information security awareness. Overall, the study showed that the level of information security awareness is high, which implies that employees of CMRs in Lagos are aware of the potential threats and risk associated with information security. Based on these research findings, recommendations were therefore made.**
Keywords: **Information Security, Awareness, Employees, Capital Market Registrars, Lagos, Nigeria**

I. INTRODUCTION

Information and information technologies have become a vital component of successful businesses and organisations. Information is being used to support every part of business, from operations to managerial decision-making and strategic competitive advantage (O'Brien, 1999). Information is one of the resources that an organisation is heavily dependent on. If the critical information of an organisation is compromised, the organisation can suffer serious consequences, that is, in the form of loss of income, loss of customers' trust and maybe legal action. Therefore, information should be protected and secured (Khan, Alghathbar, Nabi and Khan, 2011).The protection of these information assets seeks to be fulfilled by the discipline of information security. Information security is introduced into the information technology environment by implementing controls to protect against possible threats to information assets (Barnard and Solms, 2000). The controls necessary to effectively protect information assets have been influenced by technological advancement in the information technology environment. These technological advancements have brought computer processing to a wider group of

employees than ever before (Thomson, 1998). It is important in today's information technology environment that the employees are guided as to their information security responsibilities (Solms, 1998). According to Martins and Eloff (2003), guidelines and instructions of awareness are important aspects of maintaining stability. Also, Lee and Larsen (2009) affirmed that each client should be trained through stability awareness with their significant role in protecting possessed details. These are just some of the aspects of what is known as the need for information security awareness (Thomson, 1998). To ensure that an adequate level of security awareness exists within an organisation, it is important to establish an information security awareness program (ISO/IEC TR 13335‑1, 1996).

A study by Boujettif and Yongge (2010) established that 80% of major security failures are due to the poor security behaviour of the end‑users who are also their internal employees. Despite the fact that organisations have invested huge amount of money in security technology, yet user's behaviour towards information security is still weak. The effectiveness of information security can be improved if user practices recommended security behaviour. Recent efforts to address this problem take the form of awareness programs that stem directly from the policies and procedures already in place in an organisation (British Standards Institute, 1999). Policies are management instructions on the security objectives of the organisation while procedures are the specific operational steps that users must take to achieve the goals of this policy (Wood, 1994). The development of such policies and procedures is a lengthy process that requires time, money and specialised knowledge. These constraints could prove prohibitive for small to medium sized companies and is a possible cause for low level awareness in organisations. The alternative to such a company‑specific approach would be a general awareness program suitable for employees in many organisations. The main objectives of this study are; to determine the level of information security awareness among employees of CMRs within the studied area and to identify the components that influence information security awareness.

The information security will still present a difficulty for professionals and also managements. Most of the studies on information security are in nature technical and have limited emphasise on organisational and individual issues.

Nowadays, unfortunately, many organisations do not have enough consideration on individual value and so they just emphasise on technical aspects. Because of technical failures and human errors, organisations need to be aware about the necessity of educating responsible employees in order to fortify information security. In this study, employees of CMRs in Lagos have been selected as the study scope. This study will therefore attempt to examine the determinants of information security awareness among employees of CMRs in Lagos.

II. LITERATURE REVIEW

The review of literature is based on the previous studies conducted by various authors. The emphasis has been given in this section to review the literature published in various reputed international and national journal articles.

Flinn and Lumsden(2005) surveyed the user perceptions of privacy and security on the web. The study indicated that knowledge of specific technologies had a significant relationship with information security awareness. Also, Stanton, Stam, Mastrangelo, and Jolton (2005) studied analysis of end user security behaviours and found a significant effect of behaviour on information security awareness. The authors also asserted that appropriate and constructive behaviour by end users, system administrators, and others, can enhance information security effectiveness while inappropriate and destructive behaviour can substantially inhibit its effectiveness.

Kruger and Kearney (2006) developed a prototype model for measuring information security awareness in an international gold mining company. This study measured the effectiveness of information security awareness program on the basis of knowledge, attitude and behaviour. The study shows that behaviour had greater influence on information security awareness. Similarly, an empirical study by D'Arcy, Hovav, and Galletta (2009) found a significant correlation between education and information security awareness. Likewise, Siponen, Mahmood and Pahnilla (2009) affirmed that the visibility of policies play an important role in employees' compliance with organisational security policies.

Albrechtsen and Hovden (2010) conducted a study on the effects of user participation in raising security awareness through an intervention study that involved 100 employees in 6 different workshops that encouraged workshops participants to talk and discuss their opinions on information security. It shows that user participation produced changes in information security awareness and behaviour. Another study by Gordon (2010) directly determined the relationship between security awareness and security behaviour in individuals. In the same year, Takemura (2010) investigated the relationship between information security awareness and behaviour by analysing data collected from a web-based survey on information security measures in Japan and found that individuals with a high level of ISA behave significantly less problematically, in terms of organisational information security measures. The study suggested the need for improving information security education, in order to motivate Japanese workers' awareness of information security. Papagiannakis (2011) studied the current level of security awareness in Greek Companies and found that lack of clear or visible information security policy accounted for the low level of information security awareness in Greek ICT Companies.

Fakeh, Zulhemay, Shahibi, Ali, and Zaini (2012) revealed that policy of information security, education of information security, knowledge of IT, and employee's behaviour have significant influences on information security awareness. Also, Okunoye, Adebimpe, Omilabu, Olapeju, and Longe (2012) survey of information security awareness among SMEs in the South Western Nigeria showed that the problem of information security awareness is not that the personnel are not aware of information security but due to lack of pragramatic security policies and measures on the part of the organisations. The authors also recommended how the situation can be improved despite the present drawbacks.

Haeussinger and Kranz (2013) proposed a research model to study ISA's institutional, individual, and environmental antecedents and examined the mediating role of ISA. The model was empirically tested with survey data from 475 employees. The model explains a considerable proportion of the variance of ISA (.50) and intention to comply (.41). The study revealed that provision of security policies and employees' knowledge of information systems were the most influential antecedents of ISA. In the same vein, Kaur and Mustafa (2013) examined the relationship between knowledge, attitude and behaviour and information security awareness. It was found that attitude and behaviour significantly influenced confidentiality, integrity, and availability of business information.

Besides, Olalere, Waziri, Ismaila, Adebayo and Ololade (2014) carried out a research work on the assessment of information security awareness among online banking customers in Nigeria. The survey results indicated that online banking customers are not fully aware of the threats and risks associated with online banking which means that the level of information security awareness is low. However, from the above discussion, it was observed that none of the previous researchers focused on determinants of ISA among employees of capital market registrars (CMRs).

Thus, in this study, determinants of information security awareness among employees of CMRs in Lagos are investigated. Adequate knowledge about information security awareness among CMRs' employees has a direct effect on the various services rendered by the CMRs and their operations. Therefore, this study intends to enhance ongoing research efforts by exploring and identifying the determinants of information security awareness among employees of CMRs in Lagos.

III. RESEARCH HYPOTHESES

The study formulated the following research hypotheses. Simple regression analysis was employed to test the prediction power of the independent variables on the dependent variable.

1. H_1: There is a significant relationship between information security policy and information security awareness.
2. H_2: There is a significant relationship between information security education and information security awareness.
3. H_3: There is a significant relationship between knowledge of technology and information security awareness.
4. H_4: There is a significant relationship between employee's behaviour and information security awareness

IV. METHODOLOGY

Survey design was adopted for this study. The location of the study is Lagos, Nigeria. The study was limited to Lagos because of proliferation of Capital Market Registrars (CMRs) registered by Security and Exchange Commission (SEC). The population of the study comprised of CMRs' employees in Lagos. Stratified random sampling was used. The state is divided into two strata; Mainland Region and Island Region. Twelve (12) CMRs were randomly selected from the eighteen (18) CMRs within the metropolis. Total enumeration of all the staff in the selected CMRs was used for the study. Therefore, the sample size for the study was 326 respondents.

A structured questionnaire was designed to obtain necessary information from the respondents. In constructing the instrument, preference was given to previously tested questions and it followed generally accepted guidelines for building survey instruments. The questionnaire was segmented into two parts. Part A captured the demographic characteristics of the respondents. Part B captured the variables used in this study, namely information security policy, information security education, knowledge of technology, employee's behaviour and information security awareness.

To ascertain the validity of the instrument used for the study, the questionnaire went through a face validity test by an expert in the area of study, and necessary modifications were made. To further validate the instrument, a pilot test was conducted with 30 employees of CMRs in Ibadan, Oyo State.

The results of reliability test shows that all variables have good or excellent internal consistency. Abridged versions of questionnaire were personally administered by the researcher to CMRs' employees. A total of 326 questionnaires were distributed in 12 CMRs' offices in Lagos, Nigeria. Out of 326 questionnaires disseminated,

267 duly completed copies of questionnaires were returned, constituting 81.90% response rate. The duly completed questionnaires were statistically analysed using SPSS for Windows (20.0 Version).

V. ANALYSIS AND RESULTS

A. Demography of Respondents

TABLE I DEMOGRAPHY OF RESPONDENTS

Demography of Respondents(n=267)		Counts	(%)
Location	Mainland Region	150	56.2
	Island Region	117	43.8
Department	ICT	34	12.7
	Operations	112	41.9
	Marketing	35	13.1
	Finance and Accounts	48	18.0
	Admin	38	14.2
Gender	Male	116	43.4
	Female	151	56.6
Age	Under 20	0.0	0.0
	20-29	38	14.2
	30-39	159	59.6
	40-49	66	24.7
	50-59	4	1.5
	Over 59	0.0	0.0
Educational Level	Secondary	10	3.7
	Tertiary	145	54.3
	Post-Tertiary	112	41.9
Designation	Registrar/CEO	0.0	0.0
	Deputy Registrar	6	2.2
	Head of Department	52	19.5
	Officer	177	66.3
	Clerk	32	12.0
Years of Experience	0 – 5 years	69	25.8
	6 – 10 years	134	50.2
	11– 15 years	60	22.5
	Over 15years	4	1.5
Monthly Income Level	Below N50,000	22	8.2
	N50,000 – N100,000	117	43.8
	N101,000 – N150,000	48	18.0
	N151,000 – N200,000	25	9.4
	Above N200,000	55	20.6

Table I presents the result of the demographic characteristics of the respondents. The result shows that150(56.2%) of the respondents were on mainland region while island region accounted for 117(43.8%).This implies

that there are more respondents on mainland region than the island region who participated in the study. The results of the department of the respondents also reveals that 34(12.7%) were in ICT, 112(41.9%) were in Operations, 35(13.1%) were in Marketing, 48(18.0%) were in Finance and Account, and 38(14.2%) were in Admin. The result further indicates that 151(56.6%) of the respondents were females while the males were 116(43.4%).

The result shows that 159(59.6%) of the respondents were within the age bracket of 30-39 years while 4(1.5%) were within the age bracket of 50-59 years. Furthermore, the table shows that 145(54.3%) of the respondents had tertiary education, 112(41.9%) had post tertiary education, and 10 (3.7%) had secondary education. The results of the

designation of the respondents shows that 177(66.3%) were officers, 52(19.5%) were head of departments, 32(12.0%) were clerks, and 6(2.2%) were deputy registrars.

In addition, the result revealed that 4(1.5%) of the respondents had practiced for more than 15 years, 60(22.5%) had practiced for 11 and 15 years, 134(50.2%) for 6 and 10 years, and 69(25.8%) had practiced for less than 6 years. Lastly, the monthly income of the respondents revealed that 48(18.0%) earned between N101,000 and N150,000, 55(20.6%) earned more than N200,000, 25(9.4%) earned between N151,000 and N200,000, 117(43.8%) earned between N50,000 and N100,000, and 22(8.2%) earned less than N50,000.

TABLE II TESTING OF HYPOTHESES

S/N	Hypotheses	Standardised Coefficients	Significant value	Decision
H$_1$	There is a significant relationship between information security policy and information security awareness.	0.368	0.000	Supported
H$_2$	There is a significant relationship between information security education and information security awareness.	0.411	0.000	Supported
H$_3$	There is a significant relationship between knowledge of technology and information security awareness.	0.429	0.000	Supported
H$_4$	There is a significant relationship between employee's behaviour and information security awareness.	0.541	0.000	Supported

VI. DISCUSSION

The findings of the study apparently show that the level of information security awareness among capital market registrars' employees in Lagos was high. The study also was able to establish that all the highlighted factors (information security policy, information security education, knowledge of technology and employee's behaviour) significantly influenced information security awareness. The results further reveal that employee's behaviour had the highest relationship with information security awareness. This finding is in line with previous studies where policy of information security, education of information security, knowledge of IT and employee's behaviour were identified as the important elements of information security awareness amongst academic librarians in the districts of Shah Alam, Petaling Jaya, and Damansara (Fakeh *et al.,* 2012).

Based on the findings from this study, the following recommendations were made
1. Since information security policy, information security education, knowledge of technology and employee's behaviour significantly influences CMRs employees' information security awareness, the management of the CMRs must empower themselves through continuous and dedicated training and retraining for employees because awareness should be an ongoing process that incorporates every phase for growth.
2. Information security policies in the CMRs should be reviewed periodically to ensure its adequacy and conformity with the evolving environment.

3. The involvement of top management with the overall information security structure of the organisation is paramount to the effective delivery of services.
4. Finally, the CMRs managements should invest more in information security.

VII. LIMITATIONS OF THE STUDY

Like most empirical research, this study has limitations that should be taken into account. The respondents who participated in this study were basically from a single state in Nigeria. This could potentially limit the generalisability of the findings. The sample size itself is relatively small. The study can be reinforced by increasing the sample size and including participants in other geographical areas. Potential correlations between some of the independent variables (e.g. location, department, gender, age, educational level, designation, years of experience, and monthly income) need to be reported in future studies.

Since most of the impact is on employee's behaviour so considering the items of employee's behaviour are very important. Future studies can test the framework of this research in other scopes.

Besides, other study should focus on other factors that are likely to influence information security awareness among employees in CMRs. Regardless of these limitations; the findings of this study have contributed to literature in the area of information security.

Samuel Oluranti Oladipupo

REFERENCES

[1]   E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection, Anintervention study", *computers & security,* Vol. 29, pp. 432-445, 2010.

[2]   L. Barnard and R. von Solms, "A formalized approach to the effective selection and evaluation of information security controls", *Computers &Security, Elsevier Science Ltd,* Vol.19, No. 2, pp.185-194, 2000.

[3]   M. Boujettif and W. Yongge, "Constructivist Approach to Information Security Awareness in the Middle East", in Broadband*, Wireless Computing,Communication and Applications (BWCCA), 2010 International Conference*, pp. 192-199, 2010.

[4]   British Standards Institute, "Code of practice for information security management", DISC PD 0007, London, 1999.

[5]   J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information System Misuse: A DeterrenceApproach", *Information System Research,* Vol. 20, No. 1, pp.79-98, 2009.

[6]   S. K. W. Fakeh, M. N. Zulhemay, M. S. Shahibi, J. Ali and M. K. Z. Zaini, "Information security awareness amongst academic librarians", *Journal of applied sciences research*, Vol. 8, No. 3, pp.1723-1735, 2012, ISSN 1819-544X.

[7]   S. Flinn and J. Lumsden, "User Perceptions of Privacy and Security on the Web", *National Research Council,* 2005.

[8]   G. J. Gordon, "Ascertaining the relationship between security awareness and the security behaviour of individuals", Nova Southeastern: Nova Southeastern University, 2010.

[9]   F. J. Haeussinger and J. J. Kranz, "Information security awareness: Its antecedents and   mediating effects on security compliant behaviour", *34th International Conference on Information Systems 2013*, pp.1-16, 2013.

[10] ISO/IEC TR 13335-1, "Information technology - guidelines for the management of IT security – part 1: Concepts and models for IT security (First Edition)", Switzerland, 1996.

[11] F. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude and behaviouron information security awareness: A case on SME", *3rd International Conference on Research and   Innovation in Information System-2013 (ICRIIS' 13)*, pp. 286-290, 2013.

[12] B. Khan, K. S. Alghathbar, S. I. Nabi and M. K. Khan, "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management* Vol. 5, No. 26, pp.   10862-10868,   2011,   Available   online   at http://www.academicjournals.org/AJBM,DOI: 10.5897/AJBM11.067, ISSN 1993-8233.

[13] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness", *Computer & Security,* Vol. 25, No. 4, pp. 289-296, 2006.

[14] H. Kruger, L. Drevin and T. Styen, "A vocabulary test to assess information security awareness", *Information Security & Computer Security,* Vol. 18, No. 5, pp. 316-327, 2010.

[15] Y. Lee and K. R. Larsen, "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software". *European Journal of Information Systems,* 2009.

[16] A. Martins and J. Eloff, "Information Security Culture," *Proc. of IFIP TC11 17th International Conference on Information Security (SEC2002)*, IFIPConference Proceedings, Cairo, Egypt, 2003.

[17] J. A. O'Brien, "Managing information systems: Managing information technology in the internetworked enterprise (4th ed.)", United States of America, Irwin/McGraw-Hill, 1999.

[18] A. Okunoye, L.A. Adebimpe, A. Omilabu, I.O. Olapeju and O.B. Longe, "Information security awareness among SMEs in the South Western Nigeria -Significance of factors", *African Journal of Computing & ICT*, Vol. 5, No. 5, pp.184-93, 2012.

[19] M. Olalere, V.O. Waziri, I. Ismaila, O.S. Adebayo and O. Ololade, "Assessment of information security awareness among online banking customers in Nigeria", *Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, No. 6, pp.13-24,2014. ISSN: 2277 128X. Available online at: www.ijarcsse.com.

[20] K. Papagiannakis, "An overview of the current level of security awareness in companies (Master Thesis)", Erasmus School of Economics, Erasmus University of Rotterdam, pp.86, 2011.

[21] M. Siponen, M. A. Mahmood and S. Pahnila, "Are employees putting your company at risk by not following information security policies", *Communications of the ACM,* Vol. 52, No. 12, pp.145-147, 2009.

[22] J. M. Stanton, K. R. Stam, P. Mastrangelo and J. Jolton, "Analysis of end user security behaviours", *Computers & Security,* Vol. 24, No. 2, pp. 124-133, 2005.

[23] T. Takemura, "A quantitative study on Japanese workers' awareness to information security using the data collected by web-based survey", *AmericanJournal of Economics and Administration*, Vol. 2, No. 1, pp. 20-26, 2010.

[24] M. Thomson, "The development of an effective information security awareness program for use in an organization". Unpublished master's thesis, Port Elizabeth Technikon, Port Elizabeth, South Africa, 1998.

[25] R. Von Solms, "Information security management (1): Why information security is so important", *Information Management and Computer Security,* Vol. 6, No. 4, pp. 174 – 177. MCB University Press, 1998.

[26] C. C. Wood, "Information security policies made easy". Ohio: Bookmasters, 1994.