International Journal of Business and Management; Vol. 9, No. 7; 2014
ISSN 1833-3850 E-ISSN 1833-8119
Published by Canadian Center of Science and Education

Mediating Effect of Information Security Culture on the Relationship between Information Security Activities and Organizational Performance in the Nigerian Banking Setting

Mohamad Hisyam Selamat[1] & Dorcas Adebola Babatunde[2]

[1] Faculty of Business, Accounting and Management, SEGI University, Kuala Lumpur, Malaysia

[2] Department of Accounting, Universiti Utara Malaysia, Sintok, Kedah, Malaysia

Correspondence: Mohamad Hisyam Selamat, Faculty of Business, Accounting and Management, SEGI University, Kuala Lumpur, Malaysia. E-mail: mohdhisyam@segi.edu.my

Received: March 26, 2014 Accepted: May 9, 2014 Online Published: June 22, 2014

doi:10.5539/ijbm.v9n7p33 URL: http://dx.doi.org/10.5539/ijbm.v9n7p33

Abstract

The era of globalization brought about changes in the development of information technology systems, invariably affect business activities in order to be at pace with the global world (Babatunde & Selamat, 2011 & 2012). So, this paper confers on the investigation of accounting information security activities and the establishment of an information security culture in an organizational setting. The goal of this paper absolutely is to illuminate on information security projects, establishment of information security culture and the imperative of updating technological systems of the banking industry from the perspective of Nigeria as a developing country. Conversely, the challenges Nigerian banks encompassed with non-compliance with the international security standards as a result of lack of establishment information security culture, thereby led to fraud perpetration within the management. So, the governing council of Central bank of Nigeria is seeking to eradicate frauds to the minimum level. Also, the need to establish an information security culture with the organization and to update the users of technological systems meet the global world to achieve the highest key performance indicator (KPI).

Keywords: information technology, international security standard, motivation of employee and information security culture

1. Introduction

The various challenges in the era of the computer age are overwhelming, and usage of information technology is not limited to business activities but individual, homes craving for information technology are at an alarming rate. Information security objective is to leverage between the threats, vulnerabilities to information and information security and threats therein because the daily slogan is the survival of the fittest for an organization to meet up with new technologies that evolve on a daily basis. Thus, the new technological systems brought about changes to the organizational development which invariably affect business activities since information is easily assessed on the internet. Securing information could be costly. The impact of information security activities such as information technology, international security standard, information security risk, threats, and vulnerabilities, motivation of employee and perceived job roles and responsibilities and the establishment of information security culture in an organizational setting cannot be overemphasized. Hence, the need for organizations to progressively work on the information security culture establishment to keep performance indicators at the highest level through information security culture the fourth wave of information security is very imperative (Elchagar et al., 2012; Gebrasilase & Lessa, 2011). Thus, five variables discusses below relate to the establishment of information security culture that will improve organizational performance

2. Literature Review

2.1 Information Technology

The ability of organization to exploit various forms of the information technology tools such as spreadsheets, general ledger systems, are a great asset (Hurt, 2002). Information technology avails organizations to simplify operational activities such as financial report, readily available information that is timely in the banking sector

(Nickels, McHugh, McHugh, 2002). However, the issue of quality in accounting system among banks is not exclusively new, notwithstanding, there is a lack of coherent and proper implementations of the process. The banking industry still cannot meet up with the demand of the users because of the lack of accuracy and with the availability of numerous accounting softwares. So, there is a necessity for more research and development in order to meet the needs of the users accurately and timely. Thus, it is hypothesized that,

H1: Information technology is positively related to organizational performance.

2.2 International Security Standard

The trend of the British Standard Institute (BSI) certification is making waves in the Nigerian banking sector (Martins, 2012). It audits and verify bank's IS practices and compliance with international standard, it avails banks to be at par with leading international and multi-lateral corporate organizations including the International Monetary Fund and the World Bank in the area of security and protection of customers' information. Mr Onasanya (Managing Director of the First bank Plc) opined that the certification confirms that the bank has adopted and complied with the highest known management standards in information security in the world and the indication of the strength of the bank investment not only on technology, but also process and human in order to improve information security (Omu, 2010).

The international security standard (ISO) stipulates a wide range of security issues such as system policy, system compliance, physical control system organization and others (Peltier, 2003). The Nigerian banking industry has to challenge with the financial regulatory apex bodies like the Central Bank of Nigeria(CBN), Nigeria Deposit Insurance Corporation (NDIC), the Banking and Other Financial Institutions Act (BOFIA-1991), and the Accounting Standards like Accounting by Banks and Non-Bank Financial Institutions (SAS No. 10 and 15) and the International Accounting Standard on Financial Statements of Banks and Similar Financial Institutions (IAS NO.30). Thus, it is hypothesized that:

H2: International security standard is positively related to organizational performance.

2.3 Perceived Information Security Risks, Threats and Vulnerabilities

Organization need to be proactive to protect their information because of enormous increasing threats and vulnerabilities. A deep understanding of the risks will lead managers to seek for control (Straub & Welke, 1998) Threats reduce system network, and vulnerabilities enable hacking into vital information. If not addressed, it will jeopardize organizational performance (Pfleeger, 1989; Usamni, 2008; Mohammad & Suborna, 2009). The extent and nature of the information security threats and vulnerabilities are caused by the environment (Straub &Welke, 1998). Organizations are either not absolutely unprotected or even prepared to alleviate the security threats. Perceived information security policy and procedure plays a crucial part in achieving organizational strategic plans with little or no threats to information. It is hypothesized that:

H3: Perceived information security risks, threat and vulnerabilities is positively related to organizational performance.

2.4 Motivation of Employee

Motivation of employee enables employees to be highly convinced about the benefits of information security efforts towards organizational performance while rewards encourage employees to do more. In fact, employees that are motivated through benefits such as rewards and remuneration in form of bonuses, incentives, promotion, and satisfaction with conducive working environment will increase growth and organizational performance (Mozina, 2002; Rosenbloom & Hillman, 1991; Miskell & Miskell, 1991; Maslow, 1997). Thus, it is hypothesized that:

H4: Motivation of employee is positively related to organizational performance.

2.5 Perceived Job Roles and Responsibilities

Perceived job roles and responsibilities defines and clarify information security tasks for every employee, and are considered as defining factors in the information security success (Bjorck, 2001, Sami Abu-Zineh 2006). Job allocation of labor plays an important role in clarifying and defining how the responsibilities of information security are performed by the employees within the organization (Toval et al., 2002). Hence, it is hypothesized that:

H5: perceived job roles and responsibilities are positively related to organizational performance.

2.6 Organizational Performance

Performance is the outcome of the activity that has been carried out. It is also a change in the financial position of the organization as a result of activities carried out through the sound management, strong governance to achieve a better result (Sharukhalid, 2011; Cartoon, 2004). The use of performance indicator is to verify the effectiveness of information security practices and in turn information security culture is relatively new (Elchagar et al., 2012). The key objective of the organization is to increase sales volume, profit and create a niche for a competitive advantage in the global market. Human beings are the brain behind improving performance either negatively or positively. Hence, the need for establishing information security culture becomes inevitable, while the desire of the top management in the organization for information security is equally to serve as a catalyst to solve the effect of information security risks in the organization (Ransbotham & Mitra, 2009; Lohmeyer et al., 2002; Brancheau et al., 1996). Hence, it is hypothesized that:

H6: 1 information security activities are positively related to organizational performance.

H6: 2 Information security culture is positively related to organizational performance.

2.7 Information Security Culture

Culture is defined as a system of values, norms and beliefs that influence society, organizations and political systems (Robbins, 2005; Baldwin et al., 1999; Hofstede, 1997 Brown, 1995). Hofstede and Zakaria (1995 & 2007) were of the opinion that it is a learned process which could serve as motivation to the employee not only to perform but to be loyal to security practices (Hofstede, 1997; Baldwin et al., 1999; Robbins, 2005). Information security culture spells out how the employee perceives an organization. In as much as security and the risks therein are embedded in corporate culture (Kakoulidis, 2011). Thus, employees are strictly to follow the procedures and policies otherwise, rewards and punishments may be applied because the issue of information security is increasingly important (Kankanhalli et al., 2003; Brook et al., 2002).

Understanding factors that can motivate employees to diligently and sincerely implement information security activities is critical. Zakaria (2013) stated that information securities activities lead to information routines and in turn information security norms and ultimately information security culture. This continuum is illustrated in Figure 1. In other words, when discussing responsible employees in information security activities implementation, it is closely related to the establishment of information security culture within the organization.

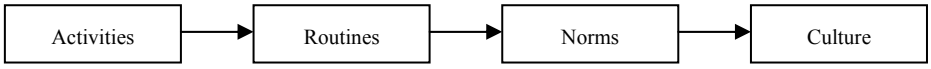

Figure 1. Information security transformation within the organization

Source: Zakaria, 2013, Babatunde, 2014.

By and large, information security culture is meant to guide the employees regarding information security threats, distortion to the objectives of security within the organization. Robbins (2005) posited that national culture; organizational culture and employees' performance are correlated. The discussion on information security culture (ISC) cannot be complete without an emphasis on organizational culture because ISC is embedded in organizational culture. Hence, Organizational Culture is defined as the backbone of efficient business value that guides and enables employees to be committed to the organization. In other words, it acts like guidance to shape the employee' behavior in order to fulfill organizational mission and vision (Denison, 1990; Schein, 1999). It is also approve the method in which employees' duties are carried out in the organization (Blake and Mouton, 1969; Schein, 1999; Lim et al., 2009). Organization establishes a security culture by motivating their staffs through training and using internal controls to obey security principles such as trust, adhering to privacy principles, and participation in security making processes and risk analyses, including management commitment to security, budget and security.

However, the impact of organizational culture on the aspect of performance improvement, information policy and managerial effectiveness cannot be over emphasizing (Claver, Llopios & Gonzalez, 2003; Gasco, 2003; Beachboard, 2004, Solm & Solm, 2004). Organizational culture helps in collaborating with the employees by providing acceptable rules and standards. In other words, it acts as a control measure that guide and shape employees' attitudes and behaviors (Lim et al., 2009). Robey and Boudreau (1999) were of the opinion that organization culture causes the resistance towards new technology and transformation while Christopian (2008) was of the opinion that it is difficult to assess organization culture in relation to knowledge management but

rather related to society or nation where the organization operates (Connar, 1997). Previous researchers postulated that there are challenges in inculcating an information security culture into the organizational culture (Knapp et al., 2006, Chia et al., 2006; Omar, 2007). Lim et al. (2009), and Fritzgerald (2007) uncovered that the organizations have the option to establish an information security culture or not. Thus, it is hypothesized that:

H7: 1 Information security culture is positively related to information security activities.

H7: Information security culture is positively related to organizational performance.

Based on the discussion above, the information security culture model is presented below in Figure 2.

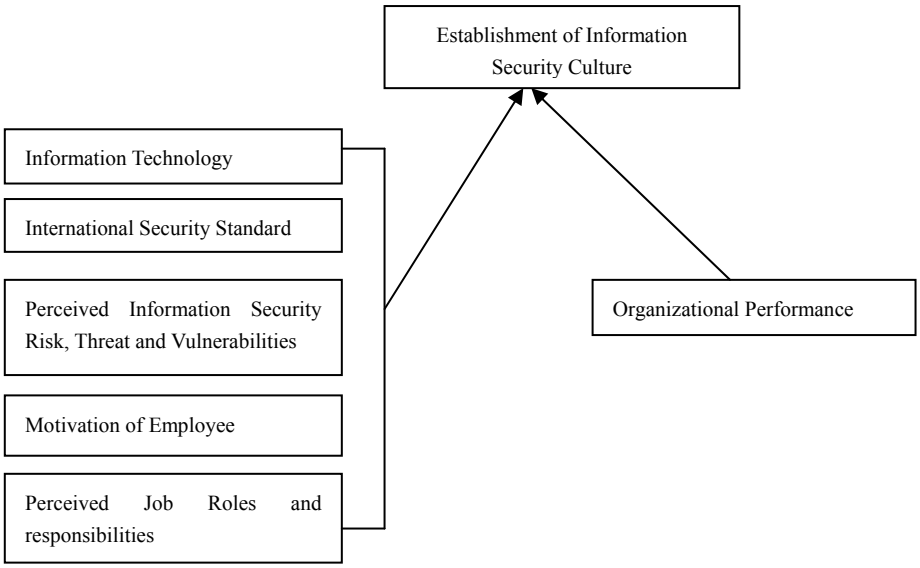

Figure 2. Information security activities and information security culture model

3. Research Methodology

The survey approach was used to test the model using questionnaires. The respondents in this study consist of (108) men and (96) women of Nigerian banks. The respondents who participated were between 25 and 55 years of age. The questionnaires were designed to get a response on the mediating effect of information security on the relationship between information security activities and organizational performance. Five point Likert scale from strongly disagree to strongly agree. Factor analysis was conducted on the seven variables measured using Likert scale to verify whether they could be treated as a single measure. The analysis was conducted using principal component analysis and varimax rotation with Kaiser Normalization.

In addition, multiple regressions were employed because it is one of the most widely used techniques in the analysis of data in the social sciences to analyze the relationship between a single dependent variable and several independent variables (Bryman & Cramer, 2001; Tabachnick & Fidell, 2001). The objective of the analysis is to predict the changes in the dependent variable in response to changes in the independent variables, whereby each independent variable is weighted by the regression analysis procedure to ensure maximal prediction from the set of independent variables (Hair et al., 1998 & 2010). The Cronbach's coefficient alpha values for the variables are presented in the Table 1 Below:

Table 1. Cronbach's alpha of all the variables

Variables	Items	Cronbach's Alpha
Information technology	4	0.764
Information security standard	4	0.758
Perceived information security risk and threat	4	0.809
Motivation of employee	3	0.712
Perceived Job roles and responsibilities	5	0.763
Organizational performance	7	0.822
Information security culture	11	0.874

4. Results of the Findings

The research model was tested using linear regression from SPSS 18 to find the strength of the relationship between the variables. From Table 1.1, the findings from regression analysis indicate that there is a strong relationship between information security activities and organizational performance when considering the alpha values. Also, the finding shows that information security activities strengthen the relationship of organizational performance. It indicates that the variables are statistically significant. Thus, the significant values are as follows: IT (β = 0.344, P value = 0.000), ISS (β = 0.162, P value = 0.018), PJRR (β = -0.126, P value = 0.047), (PISTRV (β = 0.270, P value = .000), MOE (β = 133, P value = 0.043). This result shows that IT, ISS, PJGRR, PITRV, MOE has significant impact in the relationship, hence OP improvement for competitive advantage could be made possible. The indirect relationship shows that IT (β=0.356 P value =0 .000), ISS (β= 0.166, P value=0.014), PJRR (β = -0.126, P value = 0.047), (PISTRV (β = 0.270, P value = .000), MOE (β = 133, P value = 0.043) and ISC (β = 0.036, P value = 0.021).

5. Conclusion

The era of information technology paves the way for a very highly competitive advantage the in organizational settings and information security culture establishment avails an organization to comply with security measures invariably will improve organizational performance, as a result, produce a competitive advantage in the global world (Babatunde & Selamat, 2012; Porter & Millar, 1985). Nevertheless, investing in information security culture enhance employees' compliance to security threats and presumably improve operational activities by reducing costs and as well increase profitability. This paper focuses on mediating effect of information security culture on the relationship between information security activities and organizational performance. We discussed on information security activities, such as information technology, international security standard, perceived information security risk, threat and vulnerabilities, motivation of employees, perceived job roles and responsibilities, information security culture, and organizational performance. This study laid emphasis on the fact that information security culture cannot be implemented efficiently without given attention to information security activities. In addition, the establishment of information security culture through information security activities is recognized mostly in developed countries than developing countries of which Nigeria is not exemption. The future research could consider the public sector as well as the SMEs.

References

Babatunde, D. A., & Selamat, M. H. (2012a). Investigating Information Security and its influencing Factors in the Nigerian bank Industry: A conceptual Model. *International Journal of Social Science Economics and Arts, 2*(2).

Babatunde, D. A., & Selamat, M. H. (2012b). Determining Factors Influencing Information Security Management in the Nigerian Banking and Insurance Sector: A Literature Review. *Journal of Business and Economics, 3*(6).

Brown, M., & Heywood, J. S. (2005). Performance appraisal systems: Determinants and change. *British Journal of Industrial Relations, 43*(4), 659–679.

Elchangar, H., Bouladour, B., Makoudi, M., & Regragui, B. (2012). Information Security, 4th Wave. *Journal of Theoretical Applied information Technology*, *43*(1).

Gebrasilase, T., & Lessa, L. (2011). Information security culture in public hospitals. *The African Journal of Information Systems, 3*(3).

Gupta, A., & Hammond, R. (2005). Information security issues and decision for small Business. *Information Management and Computer Security, 13*(4), 297–310.

Hong, K. S., Chi, Y. P., Louis, R. C., & Tang, J. H. (2003). An integrated System theory of Information Security Management. *Information & Management Computer Security*, *11*(5), 243–248.

Hurt, R. L. (2008). *Accounting Information System: Basic Concepts and Current Issues*. Boston: McGraw-Hill, Inc.

Krause, M., & Tipton, H. F. (2002). Handbook of Information Security. CRC Management Press LLC.

Martins, O., & Odunfa, A. (2012). At the 50th Information Value Chain Forum in Lagos.

Matins, A., & Eloff, J. (2001). Social and Ethical Aspects of Information Security.

Nickels, W. G., McHugh, J. M., & McHugh, S. M. (2002). *Understanding Business* (6th ed.). Boston: McGraw-Hill, Inc.

Odunfunwa, M. O. (2008). Impact of Information Technology on Banking Industry. *Information System Research, 12*(1).

Peltier, T. R. (2003). Preparing for ISO 17799. *Security Management Practices*, 21–28.

Porter, M., & Millar, V. (1995). How information gives you a competitive advantage. *Harvard Business Review,* 149–160.

Qingxiong Ma, Johnston, A. C., & Pearson, J. M. (2009). Implementation security management objectives and practices: a parsimonious framework. *Information Management & Computer Security, 16*(3), 251–270.

Rahman, I. (2008). The Role of Information Technology on Banking Industry: Theory and Empirics. *Nigeria Time Book Review*.

Solms, V. B. (2000). Information Security–the third wave? *Computers & Security, 19*(7), 615–620.

Von Solms, B. (2000). Information Security–The Fourth wave? *Computers and Security*, *25*(165), 165–168.

Zakaria, O. (2013). *Information Security Culture: A Human Firewall Approach.* Lambert Publishing Germany.