Association for Information Systems
AIS Electronic Library (AISeL)

MWAIS 2019 Proceedings | Midwest (MWAIS)

5-21-2019

Extrinsic Factors Influencing the Effective Use of Security Awareness Guidelines: A Comparative Study between a Bank and a Telecommunications Company

Arnold Nzailu
Dakota State University, arnold.nzailu@gmail.com

James Boit
Dakota State University, james.boit@trojans.dsu.edu

Extrinsic Factors Influencing the Effective Use of Security Awareness Guidelines: A Comparative Study between a Bank and a Telecommunication Company

Arnold Nzailu
Dakota State University
arnold.nzailu@gmail.com

James Boit
Dakota State University
James.boit@trojans.dsu.edu

ABSTRACT

Recently, the telecommunication and banking industries, regarded as key infrastructures of a country's economy, are experiencing a rapid transformation driven by changing consumer behaviors, increased competitive environment and new innovations, for example mobile technology. Thus, the purpose of this study is to investigate the influence of extrinsic factors on the behavioral decisions of users to effectively use a security awareness program. This study is quantitative in nature and explores the relationship between effective information use and other variables namely; management support, reward, punishment, social pressure, information quality and attitude. The results of the empirical testing demonstrate that information quality and attitude of employees are relevant factors towards using a security awareness program. Our results also show that reward and threat of punishment are less relevant factors.

Keywords

Banking, effective information use, extrinsic factors, telecommunication, security awareness guidelines.

INTRODUCTION

In the Democratic Republic of Congo (DRC), the banking and telecommunication sectors are the largest private employers in the nation. In the DRC, banks are regulated by the central bank and the Post and Telecommunications Regulatory Authority (ARPTC) regulates the telecommunication sector. Highly regulated industries, such as banking, are under pressure to comply with not only Congolese laws and regulations but also foreign laws and regulations such as Anti-Money Laundry Laws (AML) and Foreign Account Tax Compliance Act (FATCA). Unlike the banking sectors in the DRC that is required by the central bank to protect the information of its customers, there is no specific pieces of legislation to safeguard customer's information and privacy in the telecommunication sector. It is puzzling, therefore, that the DRC's regulatory agencies of both the banking and telecommunication sector do not require that the organizations under them to have an information security program.

This study investigated the perspective that various industries are influenced by different external factors regarding the existence of an information security program. Specifically, the differences in external influencing factors between the banking industry and telecommunication industry may explain the differences in organizational expectations relative to information security protection, thus creating variances in the effective use of security awareness program. Therefore, we formulated the following research questions; (1) What are the external factors across industries that influence employees' attitude toward information security, thus influencing the effective use of security awareness program?; (2) Does the differences in external factors influencing employees 'attitude toward security across industries attribute to the difference in the effective use of security awareness program?.

LITERATURE REVIEW

Telecommunication operators and retail banks have been converging for several years as technological barriers disappear and other extrinsic factors contribute to a further confluence. The meteoric growth of mobile phone adoption in Africa has played a great role in the acceleration of mobile banking thus penetrating the unbanked and fragmented populations that were previously isolated from accessing traditional banking products and services. For example, the innovations in mobile technology has given rise to branchless banking by extending financial services to previously neglected and unbanked

populations comprising of poor people where existing traditional banking systems were inaccessible (Ivatury and Mas 2008). Moreover, Ivatury and Mas (2008) observed that the convergence between the banking and telecommunication industry towards capturing the mobile banking market share, is in fact led by mobile operators, for example, M-Pesa in Kenya where the dominant telecommunication player Safaricom leads the mobile banking market share.

This study revisits and compares the extrinsic factors that influence effective use of security awareness programs, materials and processes in both telecom and financial industries in DRC. Unlike prior studies, this study presents a perspective from a developing nation, which is rapidly adopting newer technologies. A Congolese perspective was selected because of its largely diverse culture, and the author's knowledge of the culture. The following constructs: management support, reward, punishment, social pressure, information quality and attitude derived from different information systems theories (technology acceptance model (TAM), theory of reasoned action (TRA), general deterrence theory (GDT), and theory of planned behavior (TPB)) were leveraged to build the research model for this study.

Extrinsic motivation

Motivation is a human need, desire, an inspiration or driving force towards achieving a goal to satisfaction levels. Previous studies have identified motivation as a key factor in information technology acceptance behavior (Davis, Bagozzi and Warshaw 1992; Teo, Lim and Lai 1999; Venkatesh and Speier 1999). According to Ryan and Deci (2000), they defined extrinsic motivation (EM) as an engagement in performance goals influenced by an expected reward. Additionally, within an organizational context, Lin (2007) posits that the primary objective of EM is to receive organizational rewards. Furthermore, Padayachee (2012) suggested that an individual's behavioral characteristics influence their compliance towards information security policies.

Effective use

The effective use of information systems as an element of competitive advantage is consistently in the minds of IS managers and general managers alike. who should be cognizant of the importance of having an effective security awareness program and guidelines to mitigate the risk of potential cyber breach. Davis (Kohli and Grover 2008) argued that employees 'effective use of information in value chain activities and strategic decision making can result in improved business capabilities and/or creation of new capabilities, which then lead to better business performance. This study, therefore, will only focus on effective information use as the dependent variable and does not explicitly include business performance in the research model.

HYPOTHESES DEVELOPMENT

Information quality

Based on prior research and the context of the DR Congo, it is expected that the perceived information quality (IQ) of the security awareness program will explain whether an employee will support the program or not. Pahnila, Siponen and Mahmood (2007) found that IQ had a substantial effect on actual compliance with information security policy. Therefore, we believe that IQ will positively influence the employee attitude toward security awareness programs. Therefore, in this study, IQ refers to the relevancy, clarity, and the accessibility of the security awareness program materials. Thus, we propose our first hypothesis as follows:

H1: *Information quality will positively influence the attitude of employees towards using a security awareness program in both Banks and Telecoms.*

Management support

In DRC, evidences have shown that all the 3% allowed by laws are used for management level employees. Leonard-Barton and Deschamps (1988) argued that without observing MS at an appropriate level in the organization, it would not be useful in predicting technology acceptance behavior. In the context of this study, management support (MS) is considered the level of commitment, general support, and specific support that is demonstrated by top management in an organization. Therefore, consistent with the assertion of Guimaraes and Igbaria (1997) that MS is relevant with the greater system success and a lack of it is considered a barrier, we believe that management support will positively influence the employee extrinsic motivation

H2: *Management support will have influence on the attitude of employees towards using a security awareness program in both Banks and Telecoms.*

Reward

Pahnila et al. (2007) observed that rewards could be used as an effective means for cultivating interest and increasing motivation and performance. In the Congolese context, a reward is a monetary amount given to employees for their compliant behaviors to security guidelines. Based on previous research on incentive and rewards (Kirsch and Boss 2007; Pahnila et al. 2007) and the fact that Congolese employees and population at large still need to satisfy the lowest levels (water, electricity and, shelter) of Maslow's hierarchy of needs before advancing to the next levels , we therefore, believe that reward (RD) will positively influence the employee extrinsic motivation in this study.

H3: *Reward will positively influence the attitude of employees towards using a security awareness program in both Banks and Telecoms.*

Punishment

Based on previous works by (Barclay, Higgins and Thompson 1995) and the understanding of the Congolese culture where from childhood to adulthood, the threat of punishment has been a strong motivator for the desired result by the person in position of power. Previous studies argue that user awareness of security countermeasures reduced IS misuse intention (D'Arcy, Hovav and Galletta 2009), and the decision to commit a crime or not (Gibbs 1975) are perceived through perceived certainty, celerity and severity of sanctions. While sanctions might not be a motivator in western countries' security awareness programs, we believed that it is within the context of the DR Congo. Therefore, in this study, we believe that punishment (PU) will positively influence the employee's extrinsic motivation.

H4: *The threat of punishment of employees will have an influence on the attitude of employees towards using a security awareness program in both Banks and Telecoms.*

Social pressure

Ajzen (1991) argued that social pressure (SP) was a component of social norms (SN). Further, Herath and Rao (2009) suggested that in the context of security compliance if the employees observe their coworkers routinely following the information security practices as directed by the organization, they are likely to be inclined to carry out similar behaviors. In this study, SP is defined as the social force pushing employees to behave in a desired way. In the Congolese culture, behavior and attitude approval by peers are very highly regarded, therefore, we believe that SP will positively influence the employee's extrinsic motivation in our study.

H5: *Social pressure will have a positive influence on the attitude of employees towards using a security awareness program in both Banks and Telecoms.*

Attitude toward security

Ajzen and Fishbein (1977) argued that beliefs influence attitudes, and attitude determines the nature of intentions that guide behavioral usage. Equally, attitudes toward complying with acceptable Information Systems behaviors positively influence behavioral intentions (Bulgurcu, Cavusoglu and Benbasat 2010; Herath and Rao 2009; Myyry, Siponen, Pahnila, Vartiainen and Vance 2009; Pahnila et al. 2007). In this study, attitude toward security is defined as the degree to which an employee behaves positively or negatively toward effective usage security requirements in the organization. Therefore, we posit that a positive employee attitude will positively influence the employees effective use of security awareness guidelines.

H6: *Attitude of employees has a positive influence on the effective information use a security awareness program in both Banks and Telecoms.*

RESEARCH MODEL

The research model is shown in Figure 1. The research model is situated in capturing the extrinsic factors that influence employees' attitude toward the effective use of security awareness program in both banks and telecommunication operators.

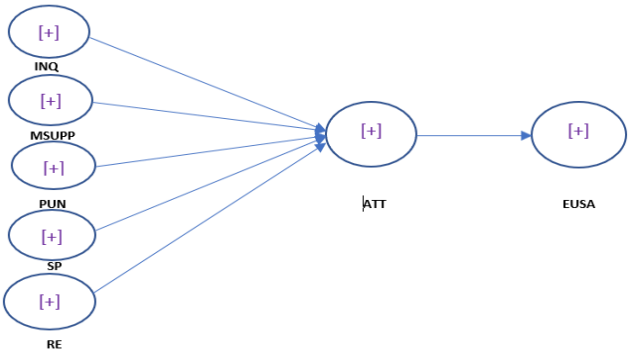

Figure 1. Research model

RESEARCH METHODOLOGY

Data collection

The data collection was conducted in a bank and a telecommunication company in the DR of Congo. A web-based survey using Likert scale (Likert 1932) was developed and used to measure the participants' beliefs and opinions toward effective use of information security program in their organization. The total number of surveys collected was 715, comprising of telecommunication company (494), and bank (221). Data was preprocessed to remove surveys (215 surveys representing 30.07% of the original 715) with missing answers to demographic and scale items.

Measurement model

SmartPLS software version 3.0, was used to run analysis of the measurement model (Ringle, Wende and Will 2005). The PLS approach allows researchers to assess measurement model parameters and structural path coefficients simultaneously (Park, Al-Ramahi and Cho 2015). Exploratory factor analysis (EFA) was also conducted to analyze and test observed indicators and underlying factors, an important step for investigating previously untested constructs. The Cronbach's alpha values, AVE scores, and composite reliability for all the reflective constructs met the 0.7 threshold, satisfying the quality criteria. With adequate factorial validity and reliability established, PLS based structural equation modeling (SEM) method was used to estimate the measurement model. Moreover, the PLS bootstrapping procedure was used to give the standardized root means square residual (SRMR) criterion. From Table 3., SRMR values were less than 0.08 (Hair Jr, Hult, Ringle and Sarstedt 2016), hence, we conclude that our model met the goodness of fit criteria. Lastly, we used PLS Multi-Group Analysis (PLS-MGA), non-parametric significance test that leverages on the PLS-SEM bootstrapping results and the results were measured at the 5% probability of error level as shown in Table 1.

RESULTS AND DISCUSSION

Performance measures

The results of this study supported the validity of the model as a useful theoretical framework that can predict user's effective use of security awareness. From Table 2., the model explained about 19% (Bank) and 25% (Telecoms) of the total variance in the dependent variable (ATT), which are respectively considered statistically weak significant (bank) and moderate significant (Telecoms). Attitude (ATT) explained about 12% (Bank) and 17% (Telecoms) of the total variance in the dependent variable (EUSA), which are considered statistically weak significant. In Table 1., we observe interesting results for H3, where the path coefficient for bank is positive while the path coefficient for telecoms is negative. On the other hand, for H4, the path coefficient for bank is negative while the path coefficient for telecoms is positive. The results empirically show that the two group of employees do differ when investigating the relationship between MSUPP and ATT, and SP and ATT.

	Path Coefficients Bank	Path Coefficients Telecom	t-Values Bank	t-Values Telecom	p-Values Bank	p-Values Telecom	Significant Bank	Significant Telecom
ATT -> EUSA	0.35	0.40	5.67	5.50	0.00	0.00	***	***
INQ -> ATT	0.30	0.26	3.72	3.48	0.00	0.00	***	***
MSUPP -> ATT	0.12	0.19	1.28	2.14	0.20	0.03	NS	**
PUN -> ATT	-0.02	0.01	0.27	0.33	0.79	0.75	NS	NS
RE -> ATT	0.12	-0.04	1.46	0.30	0.15	0.76	NS	NS
SP -> ATT	-0.03	0.15	0.73	2.13	0.46	0.03	NS	**

Table 1. Path Coefficient (Structural Model Results)

	R Square (Bank)	R Square (Telecom)	p-Values (Banks)	p-Values (Telecom)
ATT	0.19	0.25	0.00	0.00
EUSA	0.12	0.17	0.01	0.01

Table 2. R Square

	SRMR	95%	99%
Bank	0.06	0.08	0.10
Telecom	0.06	0.06	0.07

Table 3. Model Fitness

	Path Coefficients-diff (| GROUP_Bank - GROUP_Telecom |)	p-Value (GROUP_Bank vs GROUP_Telecom)	Significant
ATT -> EUSA	0.06	0.73	NS
INQ -> ATT	0.04	0.37	NS
MSUPP -> ATT	0.07	0.70	NS
PUN -> ATT	0.00	0.49	NS
RE -> ATT	0.13	0.10	NS
SP -> ATT	0.20	0.98	**

Table 4. PLS MGA

CONCLUSIONS AND EXPECTED CONTRIBUTION

This study presented a model that investigated the extrinsic factors that influence user effective use of security awareness program in both bank and telecommunication organization in the DR Congo. The research model seeks to explain the difference in the extrinsic factors that influence users' decision on effective use of security awareness program in both banking and telecom sectors. The findings suggest that the two group of employees do not differ when it comes to the relationship between ATT and EUSA (H6), INQ and ATT (H1), PUN and ATT (H4), and RE and ATT (H3). H1 and H6 were supported and positively influence the dependents variable for both groups of employees. However, H3 and H4 were not supported in this study, provoking an interesting perspective regarding a developing nation. This study contributes to the behavioral aspects of the information security body of knowledge by presenting empirical support that extrinsic factors have influence on employees' attitude toward security awareness program which in turn can predict employees' decision on the effective use of security awareness program.

REFERENCES

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational behavior and human decision processes* (50:2), pp. 179-211.

Ajzen, I., and Fishbein, M. 1977. "Attitude-Behavior Relations: A Theoretical Analysis and Review of Empirical Research," *Psychological bulletin* (84:5), p. 888.

Barclay, D., Higgins, C., and Thompson, R. 1995. *The Partial Least Squares (Pls) Approach to Casual Modeling: Personal Computer Adoption Ans Use as an Illustration*.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS quarterly* (34:3), pp. 523-548.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79-98.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1992. "Extrinsic and Intrinsic Motivation to Use Computers in the Workplace 1," *Journal of applied social psychology* (22:14), pp. 1111-1132.

Gibbs, J. P. 1975. *Crime, Punishment, and Deterrence*. Elsevier New York.

Guimaraes, T., and Igbaria, M. 1997. "Assessing User Computing Effectiveness: An Integrated Model," *Journal of Organizational and End User Computing (JOEUC)* (9:2), pp. 3-15.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., and Sarstedt, M. 2016. *A Primer on Partial Least Squares Structural Equation Modeling (Pls-Sem)*. Sage Publications.

Herath, T., and Rao, H. R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18:2), pp. 106-125.

Ivatury, G., and Mas, I. 2008. "The Early Experience with Branchless Banking," *CGAP Focus Note*:46).

Kirsch, L., and Boss, S. 2007. "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines," *ICIS 2007 proceedings*), p. 103.

Kohli, R., and Grover, V. 2008. "Business Value of It: An Essay on Expanding Research Directions to Keep up with the Times," *Journal of the association for information systems* (9:1), p. 23.

Leonard-Barton, D., and Deschamps, I. 1988. "Managerial Influence in the Implementation of New Technology," *Management science* (34:10), pp. 1252-1265.

Likert, R. 1932. "A Technique for the Measurement of Attitudes," *Archives of psychology*).

Lin, H.-F. 2007. "Effects of Extrinsic and Intrinsic Motivation on Employee Knowledge Sharing Intentions," *Journal of information science* (33:2), pp. 135-149.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study," *European Journal of Information Systems* (18:2), pp. 126-139.

Padayachee, K. 2012. "Taxonomy of Compliant Information Security Behavior," *Computers & Security* (31:5), pp. 673-680.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards Is Security Policy Compliance," *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*: IEEE, pp. 156b-156b.

Park, I., Al-Ramahi, M., and Cho, J. 2015. "The Effect of Perceived Is Support for Creativity on Job Satisfaction: The Role of Effective Is Use in Virtual Workplaces,").

Ringle, C. M., Wende, S., and Will, A. 2005. "Smartpls 2.0 (Beta)." Hamburg.

Ryan, R. M., and Deci, E. L. 2000. "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions," *Contemporary educational psychology* (25:1), pp. 54-67.

Teo, T. S., Lim, V. K., and Lai, R. Y. 1999. "Intrinsic and Extrinsic Motivation in Internet Usage," *Omega* (27:1), pp. 25-37.

Venkatesh, V., and Speier, C. 1999. "Computer Technology Training in the Workplace: A Longitudinal Investigation of the Effect of Mood," *Organizational behavior and human decision processes* (79:1), pp. 1-28.