International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 8, No.4 (July-2019)

http://dx.doi.org/10.12785/ijcds/080407

Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks

Adedayo Solomon Williams[1], Manoj S. Maharaj[1] and Adebowale I. Ojo[2]

[1] School of Management, IT and Governance, University of KwaZulu-Natal, Durban, South Africa
[2]Information Resources Management Department, Babcock University, Ilishan-Remo, Ogun State, Nigeria

Received 14 Feb. 2019, Revised 4 May 2019, Accepted 28 May 2019, Published 1 July 2019

Abstract: Information security analysts acknowledge that cyber-attacks, information theft, and internet fraud are prevalent within the banking industry. One of the issues precipitating this trend is non-compliance with standards and policies by employees. In Nigeria, employee behavioral factors that determine compliance with international information security standards and policies have not been empirically assessed. An understanding of these factors is critical in combatting cyber-related crimes, as this provides organizations with accurate information, which enables the strengthening of existing security mechanisms. An investigation into the effect of employee's behavioral factors on information security standards and policies (ISSsPs) was undertaken at selected Nigerian banks. Partial least squares structural equation modelling (PLS-SEM) was adopted for the analysis of data obtained from 370 employees of selected banks in South-West, Nigeria. The findings indicated that behavioral factors such as normative belief, security awareness, perception biases and certainty of detection positively influence employees' ISSsPs compliance. However, the severity of the penalty for non-compliance and perceived effectiveness of ISSP did not influence employees' actions.

Keywords: Information security, Standard compliance, Behavioural factors, Cybercrime

1. INTRODUCTION

Information security standards and policies provide a framework for effective management of an organization's information security. It is expected that organizations are committed to secure business practices through standards compliance. It is also indispensable that, employees of every organization comply with international information security standards and policies of their respective organizations to safeguard the assets of their organizations. Through this, organizations may apply for certification, accreditation, or a security-maturity classification attesting to their compliance with a set of rules and practices [1]. The standards considered in this paper are the Gramm Leach Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act of 1996 (HIPAA) and International Organization for Standardization (ISO).

Organizations have been advised to comply with the "Big Four" in view of ensuring information security policies and standards compliance. The "Big Four" compliances are (a) perimeter defences, (b) system certifications, (c) auditing, and (d) user involvement [2], [3]. This study is concerned with the user's involvement, specifically the banking sector employees, in information security policies and standards compliance. It was motivated by the observation that user involvement has attracted less attention, despite its significance, among Nigeria security compliance literature [4], [5].

2. PROBLEM STATEMENT

Research relating to issues of information security and cybercrime, particularly in the Nigeria banking sector, has been conducted by a number of authors [6], [7], who have mainly focused on the use of ICT in combatting fraud. For instance, studies have assessed the sociological effect of youth crime, theft and the impact of cybercrime in the financial sector of Nigeria from the perspective of employees' performance and financial losses [6]. Another study investigated the function of criminal law in preventing cybercrime, and the role of information security compliance in securing an organization's information [8]. Other empirical researches evaluated the effectiveness of information security practices in an organization [9], [10].

Although studies [4], [5], [11] have attempted to examine factors that mitigate information security compliance among the employees, gaps still exist in

E-mail: ladwillylibrary@gmail.com, maharajms@ukzn.ac.za, adebowaleojo@gmail.com

similar research that consider standards compliance in relation to Nigerian banks, particularly while considering international information security standards. The objective of this article is to determine the association between employees' behavioural factors and information security standards compliance. Some of the behavioral indices include the severity of penalty, certainty of detection, normative belief, perceived effectiveness of information security awareness and perceived bias.

3. LITERATURE REVIEW

A. Employee behavioural factors

Information security in an organization is concerned with protecting both individual, and organizational information from intruders [12]. Information security, incorporating data privacy is achieved through the implementation of suitable technology and the actions of the people responsible for the collection, collation, and storage of the data. The goal of data privacy is to protect it from unauthorized disclosure, destruction, and modification. While the technical aspects of information security are easily managed and controlled, the critically important human factor is often misunderstood and mismanaged.

Many users of information think that technology can offer full solutions to information insecurity challenges [13]. Scholars have also argued that the use of technology for information security can always yield a good result when human factors have a significant effect on computer security [12]. On the same line, the authors also suggested factors such as individual differences, cognitive abilities, and personality traits as factors that profoundly influence behavior. Similarly, studies have shown that extrinsic and intrinsic motivations influence employees' behavior to comply with information security standards [14]. Information security behavior can have a positive or negative influence on organizational culture and the information security environment. One way in which to facilitate a positive influence on information security is for employees to comply with the security standards and policies (ISSP) of their respective organizations [15]. FISMA, HIPAA, SOX, ISO 17799, and GLBA were adopted by the Nigerian banking sector. Like other financial sectors, the aim of adopting information security standards and policies is to provide necessary security to the banking information systems. It is thus important to discuss the factors that determine the employee's compliance with information security policy.

B. Employee's information security standard policy compliance (ISSsPs)

Organizational policies and standards help to secure organizational information assets when the employees and managers choose to comply with them. One of the reasons for non-compliance is the absence of clarity between the staff and management on whose responsibility information security is. A study [16] suggests that employees believe that information security protocols are counterproductive as they hinder their daily operational effectiveness. It was also observed that monitoring information security compliance by the management may be difficult. To address this, surveillance control methods have been commonly employed in many organizations [17]. The objective of behavior monitoring regarding information security compliance and governance is primarily to make sure that employees adhere to procedures, especially those that are concerned with or dealing with information security in the organization. Employees seldom adhere to information security procedures and policies. It is thus important to study employee behavior, drawing on self-efficacy theory and theory of planned behavior, which have been widely used in an organizational context.

4. THEORETICAL FRAMEWORK

A. Theory of planned behaviour

The theory of planned behaviour (TPB) by Ajzen [18] posited that human behavior is guided by three paradigms, namely: behavioral beliefs, normative beliefs and control beliefs. The behavioral beliefs consider the outcome of the behaviour and evaluate these outcomes to determine the choice of the behavior. Normative beliefs can also be referred to as subjective norms; they, on the one hand, posit that an individual will accomplish a certain task if he or she likes the higher authority in the working place. On the other hand, control beliefs relate to factors that can facilitate or mitigate the performance of the outcome of the actions. In totality, behavioral beliefs, normative beliefs and control beliefs realize positive or negative attitude toward an action; It is the combination of these behavioural paradigms that lead to behavioral intention to act, and finally, actual action/or behaviour. Behavioural intention is posited as an intermediate factor between the behavioural factors and actual behavior, and as an immediate antecedent of the behavior. This study finds the theory of planned behavior relevant as it helps in explaining employees' behavioral intention to comply with ISSsPs.

B. Self-efficacy theory

Self-efficacy theory was propounded by Bandura [19]. It is the belief that one must be motivated to complete a given task or execute an action that depends on competency. It also relates to individuals' perception of their ability to achieve a set goal. As explained by the social cognitive model, self-efficacy is dependent on behavior, environment and personal cognitive factors. These factors are said to influence each other's dynamics. Most importantly, self-efficacy is said to be the most important condition to actualize behavioural change.

In this study, aspects of the TPB and self-efficacy theory are used to construct the conceptual model in Fig 1. From the TPB and self-efficacy concepts, social influence, perceived effectiveness, and the penalty constructs were derived. It is posited that information security standards compliance is related to the perceived severity of penalty or sanction and certainty of detection. We equally propose that normative beliefs, perceived effectiveness of information security compliance and awareness of information security threats, which are imposed by subjective norms from TPB, which can be otherwise called social pressure, can increase employees' compliance with information security standards. We further propose that penalty effect is an aggregation of the perceived severity of the penalty and certainty of detection. Finally, we propose that an employee's perceived effectiveness of information security applications is related to information policy compliance.

5. CONCEPTUAL MODEL AND HYPOTHESES

The conceptual model guiding this study is shown in Figure 1. The conceptual model as well as the resulting hypotheses are discussed below. It is worthy to note that the constructs discussed were derived from past studies on information security compliance and the employee's behaviour.

A. *Severity of penalty*

In an organization, a penalty is considered a way of punishing the offender who violates the policies of the organization. It is considered the severity of punishment against committing deviant behavior [20]. They stated that severity is the degree of the sanction that will be imposed on employees that do not comply with information security policies of the organization. They also investigated employee's behavioral factor in complying with information security policy taking the severity of penalty as one of the constructs to measure the degree of compliance of the employees with deterrence theory. The authors found out that as the punishment increases, employees are less likely to comply with information security policy; and equally found out that there is a significant effect of severity of penalty on actual compliance to information security, which is in line with this study. Therefore, we hypothesize that:

H1: Severity of penalty positively influences information security standard and policy compliance.

B. *Certainty of detection*

On the one hand, the certainty of detection has been employed to know the opinion of employees on issues that bother on information security policies compliance. A study [11] showed that there is a positive and negative effect of security behavior of an employee.

This assertion posits that if employees perceived that there is a possibility of being caught when violating information security of the organization; this could motivate them to comply with the security policies. On the other hand, the severity of the penalty negatively impacts information security behavior. Some studies opined that encouragement to comply through incentive and penalties can have a negative role [21]. We, therefore, postulate that:

H2: Certainty of detection positively influences information security standard and policy compliance.

C. *Normative beliefs*

Descriptive norms refer to the degree to which one believes others are behaving. Personal belief motivates individual behavior through the possibility of having approval from others. There is the tendency that an individual may have to indirectly reciprocate the believed behavior of others. According to Hill, Fishbein, and Ajzen [22], people will develop their respective behavior which will be based on the relationship and interaction with one another. Therefore, the influence of important personality may have a persuasive influence on whether to perform a specific behavior. With respect to compliance with ISS policies and guidelines, colleagues in the workplace and manager's positive attitude towards complying with the rules may guide other people's behaviour, which will lead to a positive action [23]. The relationship between reward and actual compliance takes the normative belief as one of the contracts. The finding suggests that a significant relationship exists between normative beliefs and intention to comply. We, therefore, hypothesize that:

H3: Normative beliefs positively influence information security standard and policy compliance.

D. *Perceived effectiveness of ISS*

Behavioural studies [24], [25] have examined perceived effectiveness of ISS among home computer users. With the perceptions, computer users were found to be more likely to undertake favorable security behaviour. It has been argued that if employees believe that their actions can make a difference and have an effect on the overall organizational information security vision, they are likely to get involved in security behavior [26]. We, therefore, hypothesize that:

H4: Perceived effectiveness of ISS positively influences information security standard and policy compliance.

E. Security awareness

D'Arcy, Hovav, and Galletta [27] developed a model, which posits the user awareness of information security and the intention to misuse information of the organization. The study suggested that awareness of information security threats, perceived certainty and severity of organizational sanctions has a relationship with information security misuse. The author also suggested that awareness, which influences information security will consequently bring a reduction in information security misuse intention. We, therefore, hypothesize that:

H5: Security awareness positively influences information security standard and policy compliance.

F. Perception bias

The most prominent perception bias among employees is optimism bias. It is the belief that negative outcomes attract greater risk and that it should be given more attention [28]. It has been further described as a situation where users believe that their organizations cannot be targeted by hackers or cyber attackers [29]. This can negatively affect the employee’s intention to comply. We, therefore, hypothesize that:

H6: Perception biases positively influence information security standard and policy compliance.

G. Information security standard compliance

Standard compliance is considered as a dependent variable in this study; though sometimes, information security behaviors are dynamic, the rate of adopting information security policies and standard to handle the issues that cannot be handled by technology or automated security systems is prominent unlike before. Organizations persistently struggle with the implementation of end user’s policies. It is important to recognize the efficacy of information security standard compliance in achieving information security objectives in an organization. Moreover, several studies have extensively dealt with information security compliance [30], [31].

6. METHODS

A survey research design was adopted for the study. The population used in the study are banking employees who have knowledge about information security standard and its policy compliance. Nigerian banks are grouped into three categories, viz: first generation, second generation, and third generation. One bank was randomly chosen from each group, thus yielding a target population of 17, 916 bank employees. The Morgan theory [32] for sample size determination was used to proportionately select 370 employees from the selected banks. Three hundred and seventy (370) copies of the questionnaire were distributed, while 315 copies were retrieved, representing 85% response rate.

The instrument was developed by adopting scales from past validated studies [11] and literature on information security policy where possible. The item was developed in Likert scale measurement and worded either in past or future tense based on whether individual employees comply with information security standard of the organization. The instrument was given to experts and professionals in the field of information security to adjudge face and content validity.

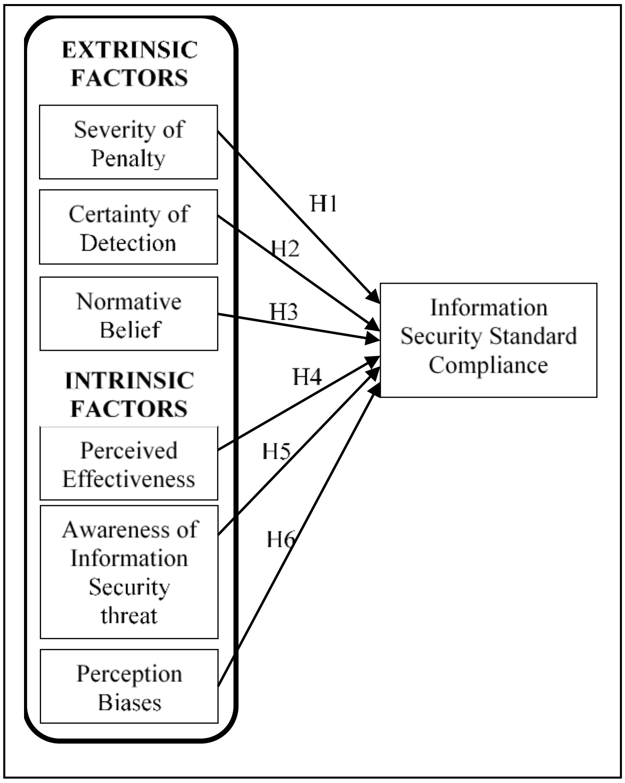


Figure 1. Conceptual Model

7. DATA ANALYSIS AND RESULTS

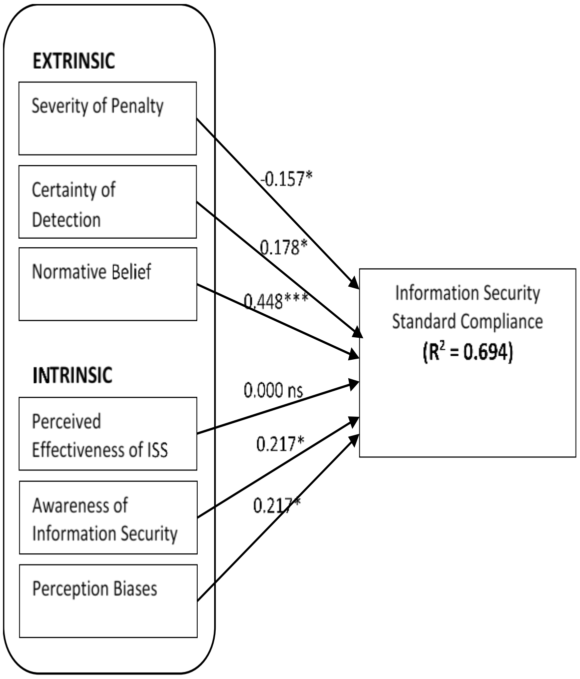
The partial least squares structural equation modeling (PLS-SEM) was adopted for data analysis with the aid of the SmartPLS3 [33] software. The PLS-SEM is a variance-based approach to structural equation modeling, and it has continued to find use in information systems research, especially in predictive models with small sample size [34], [35]. The PLS-SEM has also been used in similar studies examining factors associated with information security standard compliance [15], [36]. The first step was an analysis of the measurement model to ascertain the reliability and validity of the measures, while the second step was an assessment of the structural model to obtain the path coefficients and the coefficient of determination.

A. Assessment of the measurement model

The constructs were assessed in terms of reliability and validity. Composite reliability (CR) is used in assessing the measures' internal consistency. The CR values of all the constructs as shown in Table 1 were above 0.7, thus, indicating an acceptable measure of internal consistency [37]. Furthermore, the factor loadings associated with each item on the constructs' measure exceeded 0.70 (Table 1), thereby, demonstrating individual item reliability [38]. In establishing the model's convergent validity, the average variance extracted (AVE) was examined. The AVE value for all the constructs as shown in Table 1 were above 0.5, signifying an acceptable level of convergent validity [39]. Finally, the Fornell and Larcker [40] criterion were used in determining the measures' discriminant validity. The discriminant validity is ascertained when the square root of each construct's AVE is greater than other constructs' cross-correlations. Table 2 shows that the square root of the AVE for each construct (the principal diagonal element) exceeded the intercorrelations of the construct with other constructs in the model, thus confirming discriminant validity. The results have shown that the measurement model is psychometrically adequate for the study.

B. Assessment of the structural model

The structural model is assessed to ascertain the path coefficient (β) of the hypothesized relationships as well as the coefficient of determination (R^2). R^2 indicates the proportion of variance in the dependent variable explained by the independent variables. Also, a non-parametric bootstrapping with 5 000 resamples was conducted using the SmartPLS3 software [33] to test the significance of the model's path coefficients. The results as shown in Figure 2 and Table 3 indicate that except H3, other hypotheses raised were supported. Specifically, normative belief (β = 0.448, ρ < 0.05), security awareness (β = 0.217, ρ < 0.05), perception biases (β = 0.217, ρ < 0.05) and certainty of detection (β = 0.178, ρ < 0.05) positively influence employee's information security standard and policy (ISSP) compliance. However, while the severity of penalty (β = -0.157, ρ < 0.05) statistically influenced ISSP, it is a negative influence which is not in line with the raised hypothesis. Thus, it is supported. Also, the perceived effectiveness of ISS (β = 0.000, ρ > 0.05) did not statistically influence ISSP, thus not supported in this study. Furthermore, the model accounts for 69.4% of the variance in the dependent variable, as such, the amount of variance explained by the independent variables is substantial [34].



Path significance: * p<0.05, *** p<0.001, ns [not significant]

Figure 2. Structural model analysis and path coefficients

8. DISCUSSION

Findings from the study show that a substantial amount of variance in ISSP compliance was explained by the independent variables. Specifically, the study revealed a negative influence of the severity of penalty on ISSP compliance. This result is in line with the findings that sanctions or penalties do not have an effect on compliance with information security [31]. Herath and Rao [11], also suggested that severity of penalty has a negative impact on actual compliance to information security standard compliance. Similarly, studies [41] have argued that employing penalty for not complying with information security policy will not increase security behavior. However, this finding is contrary to that which reported that the severity of punishment increases employees' likelihood to carry out compliance attitude [11]. In the same vein, a study [42] reported that severity of punishment has a significant influence on software piracy attitude in an organization.

This study revealed that certainty of detection significantly influenced ISSP compliance. This is in line with the findings that increased certainty of detection positively influences intention to comply with organizational information security policies [11].

TABLE 1. MEASUREMENT MODEL EVALUATION

Constructs	**Items**	**Factor Loadings**	**CR**	**AVE**
Severity of Penalty	Employees caught violating security policies are appropriately corrected	0.859	0.934	0.738
	Information security policies are enforced by punishing employees that break them	0.879		
	Serial information security offenders among the employees are appropriately disciplined	0.881		
	Employees who repeatedly break security rules can lose their jobs	0.842		
	If I were caught violating organization information security policies, I would be severely punished	0.833		
Certainty of Detection	My computer practices are properly monitored for policy violations	0.842	0.920	0.697
	If I violate organization security policies, I will most likely be caught	0.870		
	My computer is monitored for security threat exposure at random times of which I am unaware	0.863		
	I am assessed for information security compliance	0.839		
	My computer is routinely checked for security threat at regular intervals in time	0.754		
Normative Belief	It is important to me for my co-workers to see me as an ethical person	0.824	0.914	0.680
	My co-workers believe I should comply with information security policy standards	0.885		
	I comply with inform security standard because my superior assesses my work	0.821		
	My co-workers believe it is important to comply with information security policy standards	0.857		
	To my knowledge, the majority of employees comply with the organization IS security policies	0.727		
Perceived Effectiveness of ISSP Compliance	Our information security policy is effective in achieving our organisational goals for information security	0.851	0.910	0.716
	Our information security policy helps to accomplish the information security objectives	0.871		
	Our information security policy keeps the risk at a minimum	0.843		
	Compliance with the requirements of the information security, reduces security risks	0.818		
Awareness of Information Security Threat	I clearly understand the implications of violating security policies	0.847	0.927	0.719
	I have received education about information security threats	0.855		
	Information regarding security threats has been communicated to me	0.859		
	I know about a continuous awareness program on general information security threat	0.848		
	Information security training was included as part of my orientation	0.830		
Perception Biases	In case of an information security threat, I always act swiftly no matter the severity of the threat.	0.822	0.927	0.680
	The measures in place to counteract information security threats are suitable and work successfully	0.840		
	The measures we use to counteract information security threats can successfully deal with the most complex of threats	0.833		
	The security-resisting mechanisms in place are successful in counteracting most threats that we experience	0.835		
	If I am unsure about a possible security threat, I prefer to take swift preventative measures rather than ignore it and have to fix it after it has happened	0.821		
	The organization sets high standards for the protection of its information assets	0.794		
ISSP Compliance	My organisation's Information security policy is consistently updated on a periodic basis	0.851	0.928	0.720
	My organisation's information security policy evolves as technology changes	0.845		
	There is a review system for our information security policy standard in my organisation	0.902		
	My organisation complies with major information security standard policies	0.853		
	Information security standard policy compliance is part of the organisation's core values	0.788		

TABLE 2. DISCRIMINANT VALIDITY COEFFICIENTS

Constructs	Constructs						
	1	2	3	4	5	6	7
Awareness	**0.848**						
Certainty of Detection	0.717	**0.835**					
ISSP Compliance	0.735	0.689	**0.849**				
Normative Belief	0.744	0.681	0.778	**0.825**			
Perceived Effectiveness	0.831	0.761	0.673	0.686	**0.846**		
Perception Biases	0.820	0.783	0.746	0.731	0.774	**0.824**	
Severity of Penalty	0.786	0.766	0.631	0.712	0.754	0.747	**0.859**

TABLE 3. PATH COEFFICIENTS

Hypothesis	β	t-value	ρ-value	Remarks
Severity of penalty -> ISSP compliance	-0.157	2.076	0.038	H1: Supported
Certainty of detection -> ISSP compliance	0.178	2.198	0.028	H2: Supported
Normative belief -> ISSP compliance	0.448	5.183	0.000	H3: Supported
Perceived effectiveness -> ISSP compliance	0.000	0.004	0.997	H4: Not supported
Security awareness -> ISSP compliance	0.217	2.336	0.020	H5: Supported
Perception biases -> ISSP compliance	0.217	2.010	0.044	H6: Supported

Furthermore, findings from the study show that normative beliefs have a significant influence on ISSP compliance. Studies [22] have shown that normative beliefs of peers, otherwise called the subjective norms of an individual, will make the individual perform the action expected. In the same vein, a study [43] revealed that individuals can be found creating their own personal behaviors based on the association with friends and colleagues. This behavior consequently influences compliance, when they see friends and colleagues in the workplace complying with ISSP of the organization; this will make them behave in the same manner. Similarly, a study [44] reported that employees' attitude toward ISSP compliance significantly influences behavioral intention toward information security compliance. With respect to security standard and policies compliance, the attitude of colleagues and managers may motivate employees to comply with the information security standard and policy. The study, therefore, suggests that colleagues and managers should lay a good example for others who will be motivated to do the same. This is in line with the self-efficacy theory adopted which suggests that one must be motivated to complete an action or a task [45]. Perceived effectiveness of information security standard compliance was also investigated and found not influencing ISSP. This is contrary to a study [31] that suggested that the quality of information security standard and policy will have an effect on actual compliance of information security. However, in this study, there is no significant influence showed. We, therefore, encourage that; other factors should be Considered by managers and senior security officers in encouraging information security compliance. Furthermore, employees should see information security standard as the policy which when followed will assist the organization to safeguard their information from intruders. In addition, the management is advised to make this impression by making the employees aware of impending danger on the non-compliance with the standard; this can be achieved through regular training of the employees of the organization.

A study [46] investigated the factors to give a precise explanation of the feature of security among the computer home users that use the wireless network. They found that there is an effect between the factors and the security threat awareness on the user computer system in line with the theory of self-efficacy theory. In agreement with this study, a study [47] found that if an individual is aware that threat to be severe, he or she will be more likely to have the intention to apply countermeasure though he or she may not even have the confidence to do that, but merely being aware of the threat will make them do so. Similarly, a study [48] agreed that perceived information security threats awareness influences positively information security policies. Likewise, awareness of information security threats to an organization's assets will likely make the employees comply with information security standard of an organization.

It was found that there is the existence of the significant influence of perception bias on ISSP, which is in line with our stated hypothesis. Also, it has been suggested that perception bias with information security standard compliance has a positive effect on ISSP [5].

Peterson [5] conducted a similar study that established the association of behavioral factors and information security policy compliance. The study found that the *severity of penalty*, the *certainty of detection, normative beliefs*, *peer behaviour*, and *perceived effectiveness* are positively associated with ISSP. We have similar constructs but added other factor that motivate the employees to comply (the *severity of penalty*, *certainty of detection* normative *beliefs*, and *perceived effectiveness, awareness of information security threats)* which are found to have significant influence on ISSP, apart from Perceived Effectiveness of ISSP which does not influence ISSP and severity of penalty that has a negative significance on ISSP. Therefore, the remaining findings supported the hypothesize.

A. *Theoretical implication*

For researchers, our article has substantially reduced problems of lack of understanding of the information security dynamic behavior of the employees and organization. To some extent, there has been some rules and guidelines adopted to improve users' behavior, which was suggested by the practitioners, but the effectiveness of the rules and guidelines has not been researched. This study has increased the suitability of using the theory of planned behavior and the theory of efficacy to explain information security standard and the behavior of the employees towards complying with information standard. Normative belief is the key factor through the application of the theory of planned behavior and self-efficacy. This consequently brings more understanding of the information security standard behavior toward the employee complying with the information standard and the condition that is attached to it. This study also has deepened our understanding of human behavior in the face of information threats.

B. *Managerial implication*

The Certainty of detection, normative belief, awareness of information security threat, and perception biases of information security threats have an influence on information security standard compliance. In this case, the IT managers and the security units must let the employees understand how serious the threats are and how they can damage the information and assets of the organization. In delivering this message, the IT managers and heads of operations must be fully involved in department meetings and seminars which could also be used to disseminate and remind the employees how crucial the information security standards compliance are and the consequences if they are not complying with the standard. It should be noted that IT managers, the heads of operation systems and the maintenance managers should endeavor to write the information security standard policies in a clear and easy-to-read language. Staffs are expected to go through information security training to increase their confidence in the ability to comply with information security and to easily identify information security threats at any time. The overall manager of the organization must ensure that all the staff are compelled to do so.

9. CONCLUSION

It is important to take information security of the organization seriously and it should not be neglected in any way and it should be known that adopting technology only as a solution to secure organization's information and assets is not enough; employee's roles are crucial. Moreover, this also calls for more research work that will stress more factors that could influence employees to comply with information security standard of the organization. This study has shown the factors that have a significant influence on ISSP through an application of self-efficacy and theory of planned behavior. It can assist the organizations in improving and implementation of information security standard compliance at the management levels and complying with the standard by the employees at the employee's level in the organization. More can equally be learned from the two theories used, as the management is trying to enforce compliance on information security in ensuring that employees take part by complying with it. Managers are expected to lay a good example to allow employees to imitate as self-efficacy suggested. This research was designed to complement the employee's self-efficacy theory and the theory of TPB in understanding ISS compliance in the banking sector.

REFERENCES

[1] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Inf. Manag.*, vol. 46, no. 5, pp. 267–270, Jun. 2009.

[2] R. Dagada and M. M. Eloff, "Integration of policy aspects into information security issues in South African organisations," *African J. Bus. Manag.*, vol. 7, no. 31, pp. 3069–3077, Aug. 2013.

[3] A. Fagerström, "Creating, maintaining and managing an information security culture," University of Arcada, Finland, 2013.

[4] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao, "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Inf. Syst. J.*, vol. 24, no. 1, pp. 61–84, Jan. 2014.

[5] M. Peterson, "Identification of Behavioral Factors within Organizations that Can Improve Information Systems Security Compliance," University of Oregon, 2014.

[6] A. Jegede, "Cyber Fraud, Global Trade and Youth Crime Burden: Nigerian Experience," *Afro Asian J. Soc. Sci.*, vol. 5, no. 4, pp. 1–21, 2014.

[7] F. Wada and G. O. Odulaja, "Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation," *Afr J Comp ICTs*, vol. 5, no. 1, pp. 69–82, 2012.

[8] Oladele John Akinyomi, "Examination of Fraud in the Nigerian Banking Sector and its Prevention," *Asian J. Manag. Res.*, vol. 3, no. 1, pp. 184–192, 2012.

[9] G. Dhillon and G. Torkzadeh, "Value-focused assessment of information system security in organizations," *Inf. Syst. J.*, 2006.

[10] D. W. Straub Jr. and R. W. Collins, “Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy,” *MIS Q.*, vol. 14, no. 2, pp. 143–156, 1990.

[11] T. Herath and H. R. Rao, “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, May 2009.

[12] K. Parsons, A. Mccormac, M. Butavicius, and L. Ferguson, “Human Factors and Information Security : Individual , Culture and Security Environment,” 2010.

[13] B. Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C,” *Gov. Inf. Q.*, 1996.

[14] K. Padayachee, “Taxonomy of compliant information security behavior,” *Comput. Secur.*, 2012.

[15] P. Ifinedo, “Understanding information systems security policy compliance : An integration of the theory of planned behavior and the protection motivation theory,” *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012.

[16] G. V. Post and A. Kagan, “Evaluating information security tradeoffs: Restricting access can interfere with user tasks,” *Comput. Secur.*, vol. 26, no. 3, pp. 229–237, May 2007.

[17] P. Adey, “Surveillance at the Airport: Surveilling Mobility/Mobilising Surveillance,” *Environ. Plan. A Econ. Sp.*, vol. 36, no. 8, pp. 1365–1380, Aug. 2004.

[18] I. Ajzen, “The theory of planned behavior,” *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, Dec. 1991.

[19] A. Bandura, “Self-efficacy: Toward a unifying theory of behavioral change,” *Adv. Behav. Res. Ther.*, vol. 1, no. 4, pp. 139–161, Jan. 1978.

[20] A. Vance, M. Siponen, and S. Pahnila, “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory,” *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, May 2012.

[21] R. Bénabou and J. Tirole, “The Review of Economic Studies Ltd . Intrinsic and Extrinsic Motivation,” *Rev. Lit. Arts Am.*, 2003.

[22] R. J. Hill, M. Fishbein, and I. Ajzen, “Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.,” *Contemp. Sociol.*, vol. 6, no. 2, p. 244, Mar. 1977.

[23] M. Siponen, S. Pahnila, and M. A. Mahmood, “Compliance with information security policies: An empirical investigation,” *Computer (Long. Beach. Calif).*, 2010.

[24] C. Anderson, “Creating conscientious cybercitizen: An examination of home computer user attitudes and intentions towards security,” in *Conference on Information Systems Technology (CIST)/INFORMS*, 2005.

[25] M. Culnan, “Bentley survey on consumers and internet security: Summary of findings,” 2004.

[26] E. Albrechtsen, “A qualitative study of users’ view on information security,” *Comput. Secur.*, vol. 26, no. 4, pp. 276–289, Jun. 2007.

[27] J. D’Arcy, A. Hovav, and D. Galletta, “User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach,” *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, Mar. 2009.

[28] L. Sjoberg, “Factors in Risk Perception,” *Risk Anal.*, vol. 20, no. 1, pp. 1–12, Feb. 2000.

[29] A. Mcilwraith, *Information Security And Employee Behaviour: How to Reduce Risk Through Employee Education, Training And Awareness*. Brookfield: Gower Publishing, 2006.

[30] M. Chan, I. Woon, and A. Kankanhalli, “Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior,” *J. Inf. Priv. Secur.*, vol. 1, no. 3, pp. 18–41, Jul. 2005.

[31] S. Pahnila, M. Siponen, and A. Mahmood, “Employees’ Behavior towards IS Security Policy Compliance,” in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)*, 2007, pp. 156b-156b.

[32] R. V. Krejcie and D. W. Morgan, “Determining Sample Size for Research Activities,” *Educ. Psychol. Meas.*, vol. 30, no. 3, pp. 607–610, Sep. 1970.

[33] C. Ringle, S. Wende, and J. Becker, *SmartPLS 3. Bönningstedt: SmartPLS*. Bönningstedt: SmartPLS, 2015.

[34] W. W. Chin, “Issues and Opinion on Structural Equation Modeling,” *MIS Q.*, vol. 22, no. March, pp. vii–xvi, 1998.

[35] C. M. Ringle, M. Sarstedt, and D. Straub, “A critical look at the use of PLS-SEM in MIS Quarterly,” *MIS Q.*, vol. 36, no. 1, pp. iii–xiv, 2012.

[36] P. Ifinedo, “Information systems security policy compliance : An empirical study of the effects of socialisation, influence, and cognition,” *Inf. Manag.*, vol. 51, no. 1, pp. 69–79, 2014.

[37] J. C. Nunnally and I. Bernstein, *Psychometric Theory*, 3rd ed. New York: McGraw-Hill, 1994.

[38] E. G. Carmines and R. A. Zeller, *Reliability and validity assessment*, vol. 17. 1979.

[39] J. F. Hair, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser, “Partial least squares structural equation modeling (PLS-SEM),” *Eur. Bus. Rev.*, vol. 26, no. 2, pp. 106–121, 2014.

[40] C. Fornell and D. F. Larcker, “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” *J. Mark. Res.*, vol. 18, no. 1, p. 39, 1981.

[41] D. W. Straub and R. J. Welke, “Coping with Systems Risk: Security Planning Models for Management Decision Making,” *MIS Q.*, vol. 22, no. 4, p. 441, Dec. 1998.

[42] A. G. Peace, D. F. Galletta, and J. Y. L. Thong, “Software Piracy in the Workplace: A Model and Empirical Test,” *J. Manag. Inf. Syst.*, vol. 20, no. 1, pp. 153–177, Jul. 2003.

[43] C. E. Aydin and R. E. Rice, “Social worlds, individual differences, and implementation,” *Inf. Manag.*, vol. 20, no. 2, pp. 119–136, Feb. 1991.

[44] N. Sohrabi Safa, R. Von Solms, and S. Furnell, “Information security policy compliance model in organizations,” *Comput. Secur.*, vol. 56, pp. 70–82, Feb. 2016.

[45] A. Y. L. Chong, F. T. S. Chan, and K. B. Ooi, “Predicting consumer decisions to adopt mobile commerce: Cross country empirical examination between China and Malaysia,” *Decis. Support Syst.*, 2012.

[46] I. Woon, G.-W. Tan, and L. R., “A Protection Motivation Theory Approach to Home Wireless Security,” in *Proceedings of the 26th International Conference on Information Systems*, 2005.

[47] B.-Y. Ng, A. Kankanhalli, and Y. (Calvin) Xu, “Studying users’ computer security behavior: A health belief perspective,” *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, Mar. 2009.

[48] Johnston and Warkentin, “Fear Appeals and Information Security Behaviors: An Empirical Study,” *MIS Q.*, 2010.

Adedayo Solomon Williams is PhD student and researcher under Professor Manoj Maharaj in the School of Management, IT and Governance, University of KwaZulu-Natal, South Africa. He bagged his master’s degree in Information Communication Technology (ICT) from the University Utara Malaysia (UUM). Previously he worked as a University Website Administrator at the University of KwaZulu-Natal Corporate Relations Office. He has equally worked as part-time lecturer at Rufus Giwa Polytechnic, Owo, Ondo State, Nigeria. His research interests are such as but not limited to information security and privacy, the economics of information security, and risk management.

Professor Manoj S. Maharaj is a Professor in the Discipline of Information Systems & Technology under the School of Management, IT and Governance, University of KwaZulu-Natal, South Africa. Prof Maharaj is an academic of more than 30 years. He has extensive experience in the management and leadership of higher education and training institutions. This includes legislation policies and procedures related to state-owned enterprises (SOEs). He has a deep knowledge of the ICT sector and has researched and published extensively in this domain. He has also contributed significantly to academic capacity development.

Adebowale Ojo lectures in the Department of Information Resources Management, Babcock University, Nigeria. He completed a postdoctoral research fellowship at the University of KwaZulu-Natal, South Africa. He obtained his doctorate in Information Resources Management from Babcock University, Nigeria. His research interests include health informatics, knowledge management, and ICT for Development.