Factors that Influence Workers' Participation in Unhygienic Cyber Practices: A Pilot Study from Nigeria

Princely Ifinedo, Nigussie Mengesha, Olumide Longe

Factors that Influence Workers' Participation in Unhygienic Cyber Practices: A Pilot Study from Nigeria

Princely Ifinedo[1[0000-0001-7032-3532]], Nigussie Mengesha [2[0000-0001-5673-5733]], and Olumide Longe[3[0000-0002-5122-3429]]

[1,2] Brock University, St Catharines, Canada
[3] American University of Nigeria, Yola, Nigeria
pifinedo@brocku.ca

Abstract. Participation or engagement in unhygienic cyber practices could ultimately harm an organization's information and communication technologies, if unchecked. This present study used concepts from the theory of planned behavior and organizational control theory to examine the effects of factors such as attitude, subjective norms, organizational facilitators, monitoring, and self-efficacy on workers' participation in unhygienic cyber practices. A cross-sectional survey of Nigerian professionals was used to test the formulated hypotheses. Partial least squares technique of structural equation modeling (SEM) was used for data analysis. The results indicate that attitude toward cyber hygiene has a negative effect on worker's participation in unhygienic cyber practices; similarly, subjective norms have a negative effect on engagement in such acts. The data did not show that organizational facilitators, self-efficacy, and monitoring had a meaningful impact on Nigerian workers' participation in unhygienic cyber practices. Implications of the study were discussed and contribution to the extant literature noted.

Keywords: Cyber Hygiene, Information Security, Employee, Survey, Nigeria.

1 Introduction

Information and communication technologies (ICT) enhance societal development and advancement across the globe [1]. Private and public organizations from Accra to Zanzibar have deployed and used ICT and other digital platforms for their activities and operations [2]. When processes and activities hinged on ICT platforms are compromised, either by non-malicious mistakes or malicious attacks, the consequences of such acts can have disastrous effects [3,4]. To ensure the safety of data resources, savvy organizations and business operators often provide workers with guidelines and instructions on how to properly use organizational ICT and other digital assets [3-6]. Prior research has examined employee ICT misuse [5], ICT abuse [4], compliance, and noncompliance with information systems (IS) security procedures [3-8]. These foregoing themes do not specifically focus on employee engagement or involvement in cyber hygiene malpractices [9,10]. Additionally, information on which factors influence or discourage participation in such behavior is not readily available in the noted studies.

The proposed research study contributes to prior research by investigating the effects of attitude, monitoring, subjective norms, organizational facilitators, and self-ef-

ficacy on employee participation in unacceptable or ill-sanctioned cyber practices. Specifically, this study is designed to address the following research questions:

a) *What is the effect of attitude toward cyber practices on employees' participation in unacceptable cyber hygiene practices*? b) *What is the effect of subjective norms on employees' participation in unacceptable cyber hygiene practices*? c) *What is the effect of organizational facilitators on employees' participation in unacceptable cyber hygiene practices*? d) *What is the effect of employees' self-efficacy regarding cyber practices on their participation in unacceptable cyber hygiene practices*? *e) What is the effect of monitoring on employees' participation in unacceptable cyber hygiene practices?*

The study is relevant because the majority of previous work in the area of end-user security behaviors has been conducted in the developed West [3-8]. Not much research has been done in Africa [11-13]. Information systems (IS) issues in advanced societies should not to be conflated with those in developing parts of the world, including Africa [11-13]. Factors that influence employee involvement in unacceptable cyber practices in Africa, with the Nigerian worker as an exemplar, may not necessarily be the same for a German or American worker. In this study, we provide a perspective of IS security management issue from a region of the world that has not been well-represented in the extant literature. Moreover, findings from a study such as this one could provide useful insights for the national cyber security frameworks recently launched in Africa, including Nigeria [14]. As well, the management of such behaviors among workers, in the region, also benefits from empirical studies of this nature. To the best of our knowledge, no previous research has explored the relationships between the effects of attitude, self-efficacy, subjective norms, organizational facilitators, and monitoring on employee participation in unacceptable cyber practices, as this present study aims to do.

2 Literature Review

2.1 Information on End User Security Behavior and Cyber hygiene

Various taxonomies on individual IS/ICT security behaviors are available in the extant IS security management literature [15-17]. For example, Magklaras and Furnell [15] discussed a model for predicting insider threats by focusing on IS misuse and abuse with examples, including data theft and stress. We build on the study by Loch et al. [16], who identified sources of information security threats to an organization, and Stanton et al. [17], who proposed a taxonomy of end-user computer security behaviors. The study focuses solely on human sources, e.g., employees and non-malicious acts. Actions of malicious entities, i.e., hackers, are outside the scope of this study, so are natural disasters, i.e., flood, fire, and so on. Stanton et al. [17] categorized the nature or acts of threats as either malicious or non-malicious. Thus, malicious end-user security behaviors include, for example, an employee who breaks into an employer's protected IS to steal trade secrets; non-malicious end-user security behaviors include items such as responding to spam email. A few researchers have investigated similar issues in developing countries, e.g., Nigeria [11-13]. For example,

Longe et al. [13] presented an overview of criminal uses of ICTs in Sub-Saharan Africa with special emphasis on the Nigerian 419 scam. Ifinedo et al. [12] reported on top non-malicious, counterproductive computer security behavior engagements among employees in Nigeria. Empirical information on workers' cyber practices and potential determinants of such in Africa are not readily available.

In essence, cyber hygiene refers to the practices, precautions, and steps users of computers and other digital devices take to maintain, safeguard, and secure data resources from intrusions and outside attacks. Here, "cyber hygiene practices" refers to the positive or favorable notion of the phenomenon while *unhygienic cyber practices* connote unfavorable and ill-advised acts. In developing an illustrative list of unhygienic cyber practices for the study (see Table 1), we consulted prior academic literature and practitioners' reports on the subject matter [6,9,10,18].

3 Theoretical Foundations

A plethora of theories have been used to explore factors affecting end-user security behaviors [19]. It is not possible to include all relevant theoretical frameworks in this preliminary study. For illustrative purposes, we will fuse common theories such as the theory of planned behavior (TPB) [20] and monitoring from the organizational control theory (OCT) [21], to understand factors that impact employee involvement in unacceptable cyber hygiene practices.

3.1 Theory of Planned Behavior

Ajzen [20] proposed the theory of planned behavior (TPB). Its three proximal predictors of behavioral intention and behavior are attitude, subjective norms, and perceived behavioral control. Attitude refers to an individual's positive or negative feelings toward engaging in a specified behavior. Subjective norms refer to an individual's perception of what people important to him/her think about a given behavior. Perceived behavioral control (PCB) refers to an individual's beliefs regarding the efficacy and resources needed to facilitate a behavior. Two sub-constructs, i.e., organizational facilitators and self-efficacy, are used to represent PCB as research shows these constructs are similar to it [8]. The former relates to resources that an organization provides to encourage or discourage engagement in a target behavior. The latter relates to an individual's ability to organize and execute courses of action required to produce/perform a specific behavior [22]. Behavior refers to an individual's observable response in a given situation with respect to a given target. For the purpose of this study, behavior is represented by unhygienic cyber practices. Several researchers have used TPB to study employee compliance with acceptable IS security behaviors and intention to use protective technologies [19].

3.2 Organizational Control Theory

Organizational control theory (OCT) is a multifaceted framework that describes the process by which one party attempts to influence the behavior of another within a given system [21]. Here, it includes management mechanisms through which an organization manages and directs the attention of its members, as well as motivates and encourages them, to act in accordance with its goals and objectives. The specific aspect of OCT considered for this present study is monitoring. Here, monitoring is the observing and checking of workers' computing practices over a regular basis. Other components of OCT, e.g., reward and specification, will be considered in future research inquires. Monitoring was chosen for this initial study because it provides an opportunity to investigate the impact of organizational efforts aimed at checking workers' adherence to prescribed IS security guidelines. Moreover, past researchers [e.g.,5] found monitoring to be relevant in understanding workers' compliance with desired IS security behaviors.

4 Research Model and Hypotheses

The study's research model is presented in Figure1. Discussions on the formulated hypotheses are provided as follows:

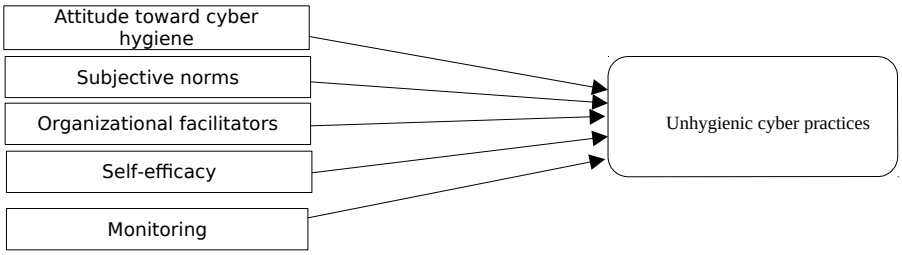

Fig. 1. The research model.

In tune with the tenets of TPB, positive attitudes influence favorable behavior and conversely, negative attitudes will diminish a target behavior [20]. Past studies show that employees who have positive attitudinal beliefs about their organization's IS security rules are the ones that readily comply with such guidelines [8,19]. Thus, it is expected that employees with positive attitudes toward cyber hygiene will have fewer compulsions to engage in unacceptable cyber hygiene practices.

H1: *Attitude toward cyber hygiene negatively affect participation in unhygienic cyber practices*.

Evidence exists to support the view indicating that an individual's behavior is influenced or motivated by what he or she observes to be the norm in his or her environment [6,20]. With regard to following acceptable organizational IS security rules, employees are more likely to adhere to their organization's ISSP if they notice that those around them, i.e., superiors, peers, and subordinates, are complying with such guide-

lines [6-8,19]. Past studies [7,8] found that subjective norms significantly affect ISSP compliance in organizations.

H2: *Subjective norms related to cyber hygiene negatively affect participation in unhygienic cyber practices*.

The availability of organizational resources facilitates a target behavior such as compliance [20]. Organizational facilitators, e.g., provision of acceptable IS use policy and the availability of IS security awareness programs, play a significant role in shaping individual perceptions of acceptable ICT use in organizations [3,5,18]. It is reasonable to expect that workers, in contexts where adequate organizational resources exist, will have less tendency to engage in ill-sanctioned computing practices and related acts.

H3: *Organizational facilitators negatively affect participation in unhygienic cyber practices*.

An individual's confidence in their knowledge and skills plays an import role in engaging in a target behavior [20]. With respect to compliance with acceptable IS security guidelines and rules, past studies demonstrated that employees with higher levels of skills and knowledge of IS security issues and consequences related to poor choices are less inclined to indulge in unfavorable ICT use practices [3,8]. Those with lower levels of knowledge do not readily follow IS security rules [23] and may knowingly or unknowingly engage in unhygienic cyber practices.

H4: *Self-efficacy negatively affects participation in unhygienic cyber practices*.

In accordance with OCT, management often evaluates and monitors the actions of employees to ensure compliance with desired goals and objectives [21]. If a worker believes that management does not monitor his/her computing practices (and their use of technologies at work), s/he is more likely to flout acceptable directives. D'Arcy et al. [5] found that when employees know that computer monitoring is in place, incidents of IS misuse drop significantly. Thus, it is expected that employees' participation in unhygienic cyber practices will likely be low if they know their organization monitors their ICT use practices.

H5: *Monitoring negatively affects participation in unhygienic cyber practices*.

5 Research Methodology

5.1 Study Design, Data Collection, and Subjects

To test the formulated hypotheses, a survey research methodology was adopted. A pilot survey was initially conducted among 25 MBA students in a local university to enhance the content and face validities of the items used for the study. Questionnaires used in the final survey were administered to working MBA students in a university in Lagos, which is the commercial capital of Nigeria; participation was voluntary. Of the 125 questionnaires distributed, 76 were returned; thus, the effective response rate for the study was 60.8%. The response rate is considered adequate for a study such as this one. Incomplete responses and poorly completed responses were excluded from subsequent data analysis. In all, 71 responses were used for the study.

Demographic information about the respondents is presented as follows: 37 are males (52.1%) and 20 are females (28.2%); the data has missing entries. Many of them (49%) have bachelor's degrees and 25% have other master's degrees. In the sample, 42.3%, 18.3%, and 15.5% of respondents were in the 21 to 30, 31 to 40, and 41 to 50 age ranges, respectively. The participants' average years of computer use is 11.5 years (standard deviations [S.D.] = 6.8) and they have 4.6 years (S.D. = 3.4) tenure at their current organizations. Some participants noted their job titles as accountant, software engineer, system analyst, project manager, internet scammer, lecturer, and customer service manager. Forty-two (42) are IT professionals and the rest are non-IT personnel. Diverse industries such as IT, manufacturing, banking, education, and so forth were represented in the sample. The data sample included an even distribution of organization size and annual revenue.

The survey collected both independent and dependent data from the same source; this could lead to common method bias (CMB) [24]. The procedures recommended to account for the effects of CMB were followed [24]. For example, respondent anonymity was assured and questions in the survey were ordered in a randomized manner. Additionally, two post-hoc statistical analyses to further reduce concerns related to the presence of CMB were used. First, Harman's one-factor test was conducted for the reflective, independent constructs. The results showed that five factors were extracted; the first factor explained 39.8% of the variance. Second, Pavlou et al. [25] suggest that an inter-construct correlation higher than 0.9 is a possible indicator of CMB. There were no correlations in Table 2 above 0.90 to further show CMB was not a problem for our data. Both tests indicated that CMB was not problematic for the collected data.

5.2 Operationalization of the Constructs

Measuring items used to represent the unhygienic cyber practices construct were taken from the following sources [6,9,10,18]. The dependent construct was modeled as a formative construct because its constituting variables measure differing phenomena.

Table 1 shows the questionnaire items used for the formative construct and their descriptive statistics. The study's participants were asked the question: "Please indicate how often you participate in the listed unhygienic cyber practices listed in Table 1." Their responses were assessed on a seven-point scale ranging from "Almost never" (1) to "Almost always" (7). The four (4) measures for attitude toward cyber hygiene, which include "Following the organization's IS security policy is a good idea", were taken constructs that have been validated [8,22]. Four (4) items for the subjective norms construct were adapted from [7,8] as well with an example: "My boss thinks that I should follow the organization's IS security policy". For the four (4) measuring items used for organizational facilitators, we used items such as "My organization has established rules of behavior for use of computer resources and other digital assets"; this was modified from [5,18]. The self-efficacy construct has items adapted from Bandura [22]; items in the construct include "I have basic knowledge on how to avoid unhygienic cyber practices." Five (5) measuring items adapted from

D'Arcy et al. [5] were used to operationalize the monitoring construct. An example includes "I believe that my organization monitors its employees' cyber practices and engagements." As indicated, the measuring items used for the reflective, independent constructs have been validated in prior studies. All the items were assessed on a seven-point scale ranging from "Strongly disagree" (1) to "Strongly agree" (7).

Table 1. Questionnaire items used for the formative construct and their descriptive statistics.

Item	Unhygienic cyber practices	Mean	SD	Weight	P-value	VIF
1	Responding to spam (i.e., unsolicited emails	3.28	2.29	+++	+++	3.879
2	Using weak passwords at work	3.63	1.92	+++	+++	4.014
3	Not updating work-related passwords regularly	3.82	2.08	0.155	0.087	2.078
4	Visiting non-related websites at work	4.05	1.69	0.115	0.015	1.285
5	Not updating anti-virus and/or anti-spyware software at work	4.15	1.96	+++	+++	4.569
6	Not logging out of secure systems after use	3.33	2.16	0.147	0.010	1.911
7	Not always treating sensitive data carefully	3.07	2.01	0.109	0.068	1.843
8	Allowing others (e.g., family) to play with work laptop	3.34	2.26	0.094	0.021	1.794
9	Downloading unauthorized software (i.e., freeware) onto work computer	3.80	2.18	0.159	0.081	1.634
10	Pasting or sticking computer passwords on office desks	2.85	2.57	+++	+++	4.963
11	Disclosing work-related passwords to others	2.95	2.38	+++	0.086	1.918
12	Leaving one's work laptop unattended	3.66	2.27	+++	0.081	2.016
13	Not backing up work files	4.38	1.81	+++	+++	3.987
14	Logging unto unsecure networks outside work, e.g., WIFI	4.19	1.90	0.153	0.09	1.666
15	Using unauthorized or personal USB at work	4.16	2.12	0.172	0.065	2.619
16	Storing work files in the cloud without authorization	3.51	2.25	0.163	0.075	1.648

Note: +++ represents entries excluded from final data analysis.

6 Data Analysis

Data analysis was done using the Partial Least Squares (PLS) technique of structural equation modeling (SEM), which is suitable for theory testing [26]. PLS supports the use of small sample sizes and does not impose data normality requirements [26,27]. WarpPLS 5.0 software was used for this study [27]. PLS supports both formative and

reflective models and recognizes two components of a causal model: the measurement and structural models.

6.1 Measurement Model

For the reflective constructs, item reliability, composite reliability, and convergent and discriminant validities were examined. Item loadings above 0.7 are recommended [26] in assessing item reliability. Item loadings from 0.700 to 0.933 were obtained for the study (they were not presented due to space limitations). Composite reliability higher than 0.707 for each construct is preferred [26]; results obtained in this regard are presented in Table 2 to satisfy this criterion. In addition, convergent and discriminant validities were assessed using the following criteria: (a) the average variance extracted (AVE) should be no less than 0.707 (i.e., the AVE should be above the threshold value of 0.50); (b) the square root of AVE should be larger than the correlations between that construct and all other constructs; and (c) the items should load more strongly on their respective constructs than on other constructs. This requirement for "c" was met but not included due to space consideration; however, information relating to the AVEs is provided in Table 2. All AVEs are above the recommended threshold of 0.50.

For the formative construct, i.e., unhygienic cyber practices, the presence of multicollinearity is checked and the item weights evaluated. Excessive collinearity within formative scales is problematic for a construct. To assess multicollinearity among the variables, the variance inflation factors (VIF) are checked. VIFs below the conservative cutoff of 3.33 are considered adequate [28]. Items weights show how significantly linked item indicators are to their specified constructs; weights with statistical significance are preferred [28]. Table 1 shows that VIFs and item weights used to capture the dependent variable are adequate. Namely, all VIFs are below 3.33 and the weights are significant at $p < 0.10$ level.

Table 1. Composite Reliability, AVEs, and inter-construct correlations.

	COM	AVE	1	2	3	4	5	6
ATT	0.85	0.59	**0.77**	0.63	0.52	-0.05	0.48	0.28
SUB	0.87	0.62	0.63	**0.79**	0.52	-0.05	0.45	0.60
FAC	0.93	0.76	0.52	0.52	**0.87**	0.06	0.55	0.34
CYB	na	na	-0.05	-0.05	0.06	na	0.16	-0.03
MON	0.91	0.66	0.48	0.45	0.55	0.16	**0.81**	0.12
SEF	0.90	0.76	0.28	0.60	0.34	-0.03	0.12	**0.87**

Note: a) COM = composite reliability; AVE = average variance extracted; b) Off-diagonal elements are correlations among constructs; c) the bold fonts in the leading diagonals are the square root of AVEs; d) ATT = Attitude, SUB = Subjective norms, FAC = Organizational facilitators, MON = Monitoring, SEF = Self-efficacy, CYB = Unhygienic cyber practice

6.2 Structural ModelF

The structural model provides information about the path significance (β) of hypothesized relationships and the coefficient of determination, squared R (R^2) [26]. Warp-

PLS 5.0 results for the βs and the R^2 are shown in Figure 2 (* indicates significance at $p < 0.5$ level). The independent variables explained 19% of the variance in the dependent variable to show the model has significant value [26]. WarpPLS 5.0 also provides information on Goodness of Fit (GoF), which is a global fit measure that accounts for both measurement and structural model performance [29]. The GoF obtained for this study is 0.33, which is close to the cut-off value of 0.36 for large effect sizes [30].

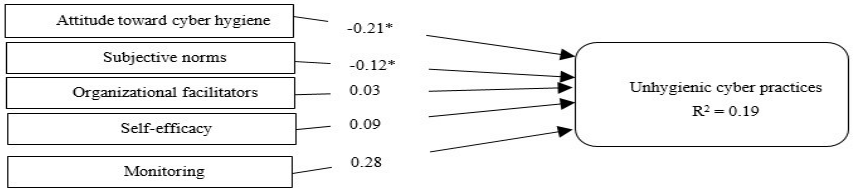

Fig. 1. The PLS result.

Consistent with H1, attitude toward cyber hygiene has a negative effect on participation in unhygienic cyber practices ($\beta = -0.21$, $p < 0.05$). H2, which predicted that subjective norms would have a negative effect on participation in unhygienic cyber practices ($\beta = -0.12$, $p < 0.05$), was confirmed as well. The data did not support H3; namely, organizational facilitators were not found to have a negative effect on participation in unhygienic cyber practices ($\beta = 0.03$, $p = 0.41$). Support was not found for H4, which predicted that self-efficacy negatively affected participation in unhygienic cyber practices ($\beta = 0.09$, $p = 0.17$). H5 was unconfirmed; monitoring was not found to have a negative effect on participation in unhygienic cyber practices ($\beta = 0.28$, $p < 0.01$). The path is statistically significant; however, the result is inconsistent with the stated prediction.

7 Discussions and Conclusion

The study's main objective was to examine the effects of relevant factors taken from TPB and OCT on workers' participation in unhygienic cyber practices. Our result confirmed that Nigerian workers with favorable attitudes toward cyber hygiene were more likely to shun participation in unhygienic cyber practices. This result supports prior studies [6-8] that showed individual attitudes towards end-user security practices are an important factor that modifies engagement in desired IS security behaviors. We found that the sampled Nigerian workers were more likely to avoid participation in unhygienic cyber practices if they believed significant others, i.e., colleagues in their workplaces, did not approve of such practices or acts. This finding is consistent with the espoused viewpoint indicating that group approval of safe and acceptable computing behaviors augurs well for compliance with the sanctioned organization's IS procedures and rules [6-8].

The result indicating that organizational facilitators mattered less for Nigerian workers with respect to their engagements in unhygienic cyber practices could be ex-

plained by contextual factors. The result is at odds with observations in a developed country that indicated that organizational facilitators help to prevent employee engagement in nonmalicious IS security acts [18]. It is possible that the sampled participants are employed in organizations where organizational resources are inadequate or lacking. For example, during an informal discussion with the researchers, one participant commented that "the attention of my company is on how to increase its market capitalization; issues like IS security is not [company X] priority." We found no meaningful association between Nigerian workers' self-efficacy and participation in unhygienic cyber practices. The result in this aspect might indicate that the sampled workers may not believe they possess sufficient skills and knowledge to help them deal with cyber issues or related practices. This might be discouraging given that past studies [6-8,19] from developed countries have shown that adequate levels of skills, capabilities, and knowledge of end-user IS security issues are pertinent for suppressing involvement in ill-sanctioned computing behaviors. It is somewhat surprising that the relationship between monitoring and the dependent construct was unsupported in our research setting. Prior IS security studies that used monitoring found it to be an important mechanism for shaping behavioral intentions to comply with acceptable rules [5]. Our result shows that more monitoring seems to lead to more participation in unhygienic cyber practices. A plausible explanation for the lack of support for H5 might be due to extraneous factors. For example, it is possible that the sampled participants are unperturbed by IS security directives and monitoring in their organizations or are able to circumvent such efforts through neutralization techniques [31]. To some degree, their profession or occupation might also have an influential role. Recall most of the study's participants are IT professionals and four (4) of them candidly indicated they are internet scammers. Evidence exists to show that employees likely to flout organizational IS security directives are those with more advanced IT know-how [3].

7.1 Contributions to Research and Implications for Practice

This study is one of the first of its kind to investigate worker's participation in unhygienic cyber practices by using perspectives from TPB and OCT. No previous study has considered the effects of the selected variables on the dependent construct with data collected from Africa. This study offers support for the applicability of TPB and OCT in understanding employee participation in unhygienic cyber practices in work settings. Findings of the study lend credence to prior studies emphasizing the roles of attitudinal beliefs and subjective norms in shaping desired behaviors. There are implications of the study's findings for practice, in particular, the management of workers in Nigeria in relation to their discouraging participation in unhygienic cyber practices in work environments. Management can better control workers' behaviors with respect to the phenomenon by proactively providing incentives (e.g., campaigns, training) that can enhance positive attitudes towards favorable cyber hygiene practices. Well-tailored communication could also influence attitudes toward desired behavior.

Given the importance of subjective norms in reducing employees' engagement in unhygienic cyber practices, management should ensure concerns related to acceptable cyber practices are regularly discussed at department meetings and widely situated in

the social functioning of the enterprise. Influential persons in the organization could be given the responsibility to act as “champions” of the cause of promoting good cyber hygiene practices [7]. It is likely that the amount of variance explained in the research model could increase further if more favorable organizational facilitators are made available to workers. Similarly, identifying specific measures that can enhance worker’s self-efficacy in relation to cyber practices could help produce more fruitful results. Reliance on monitoring mechanisms may not be totally effective in a context where workers possess above average ICT/IS knowledge; deterrence and sanction mechanisms may be needed to ensure compliance [4,7].

7.2 Study’s Limitations and Future Research Directions

There are several limitations to this study. First, the data came from a cross-sectional field survey; longitudinal data may facilitate more insight. Second, the data was obtained from Nigerian workers. Findings in this preliminary study may not be applicable to workers in other parts of Africa; perceptions may vary across the continent. Third, the sample is small. Fourth, although CMB was not problematic for this study, it is still possible that participants might have provided “socially desirable responses” [24] to some of the issues being investigated. Future studies could overcome the noted shortcomings in this study. Comparative studies on the continent and elsewhere could be conducted. Attention should be paid to other end-user security behaviors such as those related to malicious acts. Other aspects of OCT, e.g., reward, could be explored. Likewise, other relevant theories in the area of IS security management [19] could be used to study the phenomenon and case studies could be used to enhance insights.

References

1. Niebel, T.: ICT and economic growth – Comparing developing, emerging and developed countries. World Development 104, April 2018, 197-211 (2018).
2. Haftu, G.G.: Information communications technology and economic growth in Sub-Saharan Africa: A panel data approach. Telecommunications Policy, in press (2018).
3. Ifinedo, P.: Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. Information Resources Management Journal 31(1), 53-82 (2018).
4. Hu, Q., Xu, Z., Dinev, T. and Ling, H.: Does deterrence work in reducing information security policy abuse by employees? Communications of the ACM 54(6), 54-60 (2011).
5. D’Arcy, J. P. and Devaraj, S.: Employee misuse of information technology resources: testing a contemporary deterrence model. Decision Sciences 43(6), 1091-1124 (2012).
6. Guo, K. H., Yufei, Y., Archer, N.P. and Connelly, C.E.: Understanding nonmalicious security violations in the workplace: a composite behavior model. Journal of Management Information Systems 28(2), 203–236 (2011).
7. Ifinedo, P.: Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Information & Management 51(1), 69-79. (2014).

8. Bulgurcu, B., Cavusoglu, H. and Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3), 523-548 (2010).
9. Aldorisio, J., What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More, https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more, last accessed Aug 20, 2018.
10. CITI, Clearswift Insider Threat Index (CITI). US Edition. http://pages.clearswift.com/rs/591-QHZ-135/images/Clearswift_Insider_Threat_Index_2015_US.pdf, last accessed Jan 7, 2017
11. Njenga, K. and Brown, I.: Conceptualising improvisation in information systems security. European Journal of Information Systems 21(6), 592-607 (2012).
12. Ifinedo, P., Longe, O. B., and Amaunam, I.: Top exemplars of non-malicious, counterproductive computer security behaviours (CCSB) engagements among employees in Nigeria: recommendations for management. In: the 8th iSTEAMS, pp. 5-12, Lagos, Nigeria (2017).
13. Longe, O., Ngwa, O., Wada, F., Mbarika, V., and Kvasny L.: Criminal uses of information & communication technologies in sub-Saharan Africa: Trends, concerns and perspectives. Journal of Information Technology Impact 9(3), 155-172 (2009).
14. Technology Times, Nigeria adopts framework for national security policy, https://technologytimes.ng/nigeria-adopts-framework-national-cyber-security-policy/, last accessed Aug 20, 2018.
15. Magklaras, G. B., and Furnell, S. M.: Insider threat prediction tool: evaluating the probability of IT misuse. Computers & Security 21(1), 62-73 (2002).
16. Loch, K. D., Carr, H. H. and Warkentin, M. E.: Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly 16(2), 173-186 (1992).
17. Stanton, J.M., Stam, K.R, Mastrangelo, P. and Jolton, J.: Analysis of end user security behaviors. Computers & Security 24(2), 124-133 (2005).
18. Ifinedo, P. and Cashin, J.: Using social cognitive theory to understand employees' counterproductive computer security behaviors (CCSB): A pilot study. In: The 27th International Business Research Conference (IBRC), Toronto, Canada (2014)
19. Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Information Management and Computer Security 22(1), 42–75 (2014).
20. Ajzen, I.: The theory of planned behavior. Organizational behavior and human decision processes 50(2), 179-211 (1991).
21. Eisenhardt, K.M.: Control: Organizational and economic approaches. Management science 31(2), 134-149 (1985).
22. Bandura, A.: Social foundations of thought and action: A social cognitive theory. Prentice-Hall, Englewood Cliffs, NJ (1986).
23. Yazdanmehr, A. and Wang, J.: Employees' information security policy compliance: a norm activation perspective. Decision Support Systems, 92, 36-46 (2016).
24. Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. and Podsakoff, N. P.: Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of Applied Psychology 88(5), 879-903 (2003).
25. Pavlou P.A., Liang H. and Xue Y.: Understanding and mitigating uncertainty in online exchange relationships: a principal-agent perspective. MIS Quarterly 31(1), 105–136 (2007).
26. Hair, J.F., Tomas, G., Hult, M., Ringle, C.M. and Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Sage, Thousand Oaks, CA (2014).
27. Kock, N.: WarpPLS 5.0 User Manual, ScriptWarp Systems, http://cits.tamiu.edu/WarpPLS/UserManual_v_5_0.pdf, last accessed February 27, 2017.

28. Petter, S., Straub, D., and Rai, A.: Specifying formative constructs in information systems research. MIS Quarterly 31(4), 623-656 (2007).
29. Tenenhaus, M., Vinzi V.E., Chatelin Y-M and Lauro, C.: PLS path modeling. Computational Statistics and Data Analysis 48(1), 159-205 (2005).
30. Wetzels, M., Odekerken-Schröder, G. and Van Oppen, C.: Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. MIS Quarterly 33(1), 177-195 (2009).
31. Siponen, M., A. and Vance, A.: Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly 34(3), 487-502 (2010).