Top Exemplars of Non-Malicious, Counterproductive Computer Security Behaviours (CCSB) Engagements Among Employees in Nigeria: Recommendations for Management

Ifinedo, P.
Department of Finance and Information Management
Cape Breton University, Canada
princely_ifinedo@cbu.ca
+1 902 563 1227

Longe, O.B
Caleb Business School
Caleb University
Imota, Lagos State, Nigeria
longeolumide@calebuniversity.edu.ng
+2348160900893

Amaunam, I.
Department of Computer Science
Akwa Ibom State University
Ikot Akpaden, Nigeria
aideeamaunam@gmail.com
+2348063596298

ABSTRACT

Benign, non-malicious computer security practices that employees across the globe participate in can cause organizations serious problems just as much as malicious security acts. Not much research has been done in this aspect of information security management in Nigeria. It is worth noting that studies of cyber threats are readily available. In this study, we focused specifically on counterproductive computer security behaviours (CCSB), which is a growing phenomenon worldwide. Essentially, CCSB are ill-prescribed computer use practices and general information security behaviours that go against the legitimate interests of an organization. In that regard, we collected empirical data from organisational actors (i.e., employees) in Nigeria regarding their views on the phenomenon. Subsequently, we ranked their responses on issues we sampled. Discussions on the top five exemplars of CCSB were presented and recommendations for ameliorating these concerns were provided for management. We hope the insights offered by our study will benefit both practice and theory in the area.

Keywords: Information systems (IS) security, Counterproductive computer security behaviours, Non-malicious, Employees, IS security management, Nigeria, Survey, Mean ranking.

Article Citation Format
Ifinedo, P., Longe, O.B. & Amaunam, I. (2017): Top Exemplars of Non-Malicious, Counterproductive Computer Security Behaviours (CCSB) Engagements Among Employees in Nigeria: Recommendations for Management. Proceedings of the 8th iSTEAMS Multidisciplinary Conference, Caleb University, Lagos, Nigeria. Pp 5-12.

1. BACKGROUND TO THE STUDY

Organisations use various computer networks and information systems (IS) to hold valuable organisational data assets and resources (Davenport & Short, 1990, Ifinedo, 2014). Information-related resources are considered to be among the most valuable assets held by any organisation (Kamoun and Nicho, 2014). Threats to an organisation's IS resources and digital assets can emanate from within or outside its boundary (Ifinedo, 2009, Crossler et al, 2013, Posey et al., 2013). It is not surprising to see that organisations tend to marshal resources against threats from outside; however, studies show that a substantial proportion of information security threats actually originate from inside the organisation (Stanton et al., 2005, Bulgurcu et al, 2010, Posey et al, 2013). An example of human agents is the organisation insider who could pose a dangerous threat to organisational information systems (IS) than outsiders' actions (Posey et al., 2013). This is because insiders often have intimate knowledge of organisational informational assets as they use such systems and applications for routine work activities.

The human agent (i.e., employees), either intentionally or unintentionally engages in ill-prescribed behaviours and practices that can endanger organisational IS resources (Stanton et al, 2005, Vance et al, 2012, Ifinedo, 2014). One example of ill-prescribed behaviours is counterproductive computer security behaviours (CCSB), which refers to employees' computer use practices and general information security behaviours that go against the legitimate interests of an organisation (Ifinedo & Akinnuwesi, 2014). Examples of CCSB considered in our study include visiting non-related websites at work, not updating work-related passwords regularly, and disclosing password to others.

Organisations advocate acceptable computing behaviours through a variety of policies (e.g., ethical computer use policy, acceptable use policy, email use policy, social media policy). In the context of this study, CCSB would be any practices or acts engaged by organisational members that diverge from recommended guidelines and policies. Oftentimes, organisations across the world spend millions of dollars to control IS security threats posed by employees who are seen as a major concern in the IS security chain (Ifinedo, 2009, 2014) because of their tendency to deviate from acceptable IS security guidelines. To this end, research on employee participation in IS security misbehaviour, including CCSB is both time and necessary.

Counterproductive Computer Security Behaviours (CCSB)

In developing the CCSB items considered in this study, we consulted prior literature dealing with such issues (Crossler et al, 2013, Guo et al, 2011, Vance et al, 2010, Posey et al, 2013, Loch et al, 1992, Stanton, et al, 2005). In particular, the classification presented in (Loch et al, 1992, Stanton, et al, 2005) was considered pertinent to this study. Loch et al. (1992) identified sources of information security threats to an organisation, and Stanton et al. (2005) proposed a taxonomy of end-user security risk behaviours as either malicious or non-malicious. In brief, CCSB is an active, volitional act that excludes malicious end-user security risk behaviours. Figure 1 illustrates the IS security vector conceptualization. The path of concern to this study is indicated by an arrow, and the box with broken lines depicts CCSB. This scheme is modified from Loch et al. (1992).

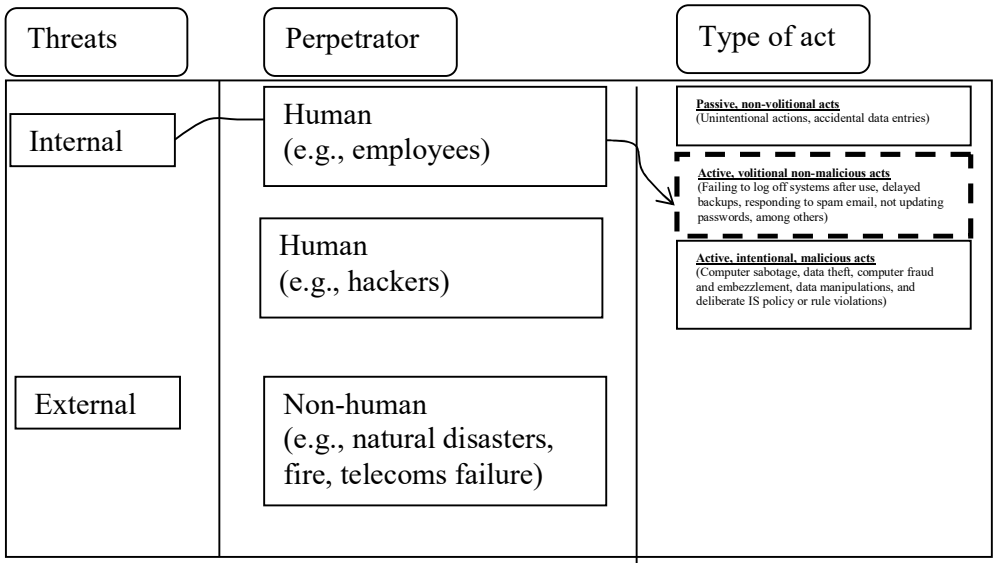

Figure 1: Conceptualization of the IS security vector

After searching the relevant literature and engaging in a series of discussions with IS security practitioners and IS professors, we drew up a list of CCSB items, which was pared down to 12 items for illustration purposes (Table 1). Another study discussing how the selected CCSB items were chosen as examples of commonly practiced CCSB in organisations is to appear elsewhere. The items in Table 1 depict insider, non-malicious end user security behaviours (Posey et al, 2013, Loch et al, 1992, Stanton, et al, 2005). Examples of non-malicious CCSB considered indicated herein include the following items: "failing to log off when leaving PC", "allowing children to play with laptop" and "sharing passwords" were sourced from the literature (See also Posey et al, 2013, Vance et al, 2012, Ng et al, 2005).

Table 1. The List of CCSB Considered in the Study

No.	Ref.	CCSB
#1	CCSB1	Responding to spam (i.e. unsolicited emails)
#2	CCSB2	Using weak passwords at work
#3	CCSB3	Not updating work-related passwords regularly
#4	CCSB4	Visiting non-related websites at work
#5	CCSB5	Not updating anti-virus and/or anti-spyware software at work
#6	CCSB6	Not logging out of secure systems after use
#7	CCSB7	Not always treating sensitive data carefully
#8	CCSB8	Allowing one's family (i.e. children) to play with work laptop
#9	CCSB9	Downloading unauthorized software (i.e. freeware) onto work computer
#10	CCSB10	Pasting or sticking computer passwords on office desks
#11	CCSB11	Disclosing work-related passwords to others
#12	CCSB12	Leaving one's work laptop unattended

2. STATEMENT OF PROBLEM

The majority of studies in the area of end user security behaviours have been conducted in the developed West (Crossler et al, 2013). Information from the developing parts of the world, including Nigeria is rare in the extant literature (Ifinedo and Akinnuwesi, 2014). Past researchers argue that it is rewarding for IS and information technology (IT) issues in advanced societies not to be conflated with those in developing parts of the world. This is because diffusion of technological innovations, acceptance of IS security and privacy practices, indulgence in antisocial computer practices, and so forth have been known to differ by regional locations or contexts (Gregorio et al, 2005, Comin, et al, 2010, Bagchi et al, 2006, Ifinedo, 2009).

While several prior studies have focused mainly on employees' IS policy violations in organisations (Hu et al, 2015, D'Arcy et al, 2009), misuse of IS resources and unethical IS use behaviour (D'Arcy et al, 2009, D'Arcy & Devaraj, 2012, Leonard et al, 2001), to date, not many researchers have specifically focused on issues in developing countries, including Nigeria those that did only paid attention to malicious, cyber security threats and crimes (Alese et al, 2014, Longe & Chiemeke, 2008, Ibikunke & Odunayo, 2013, Oyelere & Oyelere, 2015). The current study is designed to enlighten on employee participation in CCSB.

3. OBJECTIVE

The main objective of this study is to explore and rank how employees in Nigeria perceive the problem of CCSB. The five top issues will be identified and discussed in manner congruent with key IS issues studies in the IS literature (see, Ifinedo, 2006).

4. METHODOLOGY

4.1 The Research Design

We wish to state that this current study is a part of a larger research on the assessment of CCSB across national contexts. We used a field survey to gather relevant information from all contexts, including in Nigeria. The survey was administered through a research company. Nigerian business professionals from diverse industries with knowledge of CCSB were contacted. The research company gave their panel members points-based incentives redeemable for prizes. The criteria for including participants in the survey are: a) knowledge of CCSB, and b) employment in an organisation. The research company's web server reported that 1300 Nigerian respondents were invited of which 728 opted to participate in the survey by accepting the consent agreement. The survey was designed such that respondents who indicated indulging in less than 5 CCSB in the last 6 months were prevented from continuing to the next step. Recruiting participants with more knowledge and engagements in CCSB, we hoped, benefits our cause more than do those with limited involvement and knowledge of the phenomenon. In total, 451 panels were dropped, and of the 277 responses, only 81 were considered useable.

Broadly, responses that included monotone or patterned responses, many missing answers, and generally, badly completed surveys, were removed. Overall, the data was checked for violations of assumptions i.e. normality and linearity; the results indicated that these assumptions were met.

In our study, we asked participants to indicate how often they have indulged in the CCSB listed in Table 1. Their responses were assessed on a 7-point Likert scale ranging from “Almost never” (1) to “Almost always” (7).

5. DATA PRESENTATION

Data were entered into statistical package for social sciences (SPSS) ver 22. Data analysis used descriptive statistics. The mean for each CCSB was tabulated and ranked.

Table 2: Mean Score and Ranking of CCSB

CCSB	Mean (SD)	Rank
Responding to spam (i.e. unsolicited emails)	2.7 (1.7)	9
Using weak passwords at work	3.2 (1.7)	6
Not updating work-related passwords regularly	3.3 (1.9)	5
Visiting non-related websites at work	4.3 (1.7)	1
Not updating anti-virus and/or anti-spyware software at work	3.6 (2.1)	3
Not logging out of secure systems after use	3.8 (2.1)	2
Not always treating sensitive data carefully	2.3 (1.7)	10
Allowing one’s family (i.e. children) to play with work laptop	2.8 (2.1)	7[a]
Downloading unauthorized software (i.e. freeware) onto work computer	3.4 (1.9)	4
Pasting or sticking computer passwords on office desks	1.9 (1.6)	12
Disclosing work-related passwords to others	2.0 (1.7)	11
Leaving your work laptop unattended	2.8 (1.4)	7[a]

a. *A tie in the mean score; SD = standard deviation*

6. DISCUSSION OF FINDINGS

The ranking of the CCSB items are provided in Table 2. The top 5 CCSB items are: 1) Visiting non-related websites at work, 2) Not logging out of secure systems after use, 3) Not updating anti-virus and/or anti-spyware software at work, 4) Downloading unauthorized software (i.e. freeware) onto work computer, and 5) Not updating work-related passwords regularly. Each of the top five CCSB is discussed next and recommendations for managing each concern is provided. The full list will be discussed elsewhere.

1) Visiting non-related websites at work

Workers' productivity is affected when they employees routinely visit non-work related websites at work. The problem is not limited to Nigerian workers. For example, Conner (2012) reported the findings in a survey in a developed country which showed that "64 percent of employees visit non-work related websites every day at work" and this problem had a negative effect on workers' efficiency. To address this concern, management could consider implementing employee monitoring tools and applications capable of logging worker's daily activities on the Internet. Such tools can provide information on how long workers use Social Network websites (like Twitter) at work. How long employees spend time on the Internet and what amounts of time was spent for personal business. Deploying monitoring must be done in an ethical and legal manner.

2) Not logging out of secure systems after use.

Some have reported that workers in Nigerian organizations often leave IS and computers unattended in work environments. Instead of logging out of computer systems, some employees prefer to keep the session running. Such practices expose computer systems to attacks. Frank and Odunayo (2013) report on some of the challenges posed by such behaviours. To ameliorate this, the following are recommended:

i. (i)Educate system users: A large section of the Nigerian society is not well-informed of acceptable computing practices and rules. An average computer user in the country lacks understanding of the vulnerabilities posed unattended systems. Thus, it is necessary for management to organize workshops, seminars, and training sessions to educate users of the dangers of such actions.
ii. (ii) System tracking: Another way of tackling this particular problem is to develop and install applications and software that could track and logs off a workstation if found to be idle for a long time.
iii. (iii) Grant administrative privileges: Certain privileges should be granted to trained administrators who can access idle systems and log them off them if found to be idle for too long.

3) Not updating anti-virus and/or anti-spyware software at work

A lot of system users in Nigeria do not understand the importance of installing antiviruses or antispyware let alone updating such software. Users' understanding of the IS/IT and the sorts of issues that could pose threats to such systems are still evolving in Nigeria. Oyelere and Oyelere (2015) noted a lack of knowledge in such matters can create a lot of problems for an organisation. To reduce this problem, the following approaches could be adopted:

i. Educate the users: There is a need to provide education and training in such areas. For example, informing all organisational actors of the relevance of antiviruses/antispyware and how to install them as well as update such tools are worthy of attention.
ii. Assigning roles: Certain system administrators in the organisation could be tasked to do the job of updating anti-virus and/or anti-spyware software on a regular basis.
iii. Configure a gateway update server: An alternative cause of action could be instituted, e.g., signature servers could be configured to handle the processes by setting up and updating anti-virus and/or anti-spyware software tools at work form a centralized point.

4) Downloading unauthorized software (i.e. freeware) onto work computer

Hackers often try to gain access to an organisation's IS and computer network by attaching malware to freeware that are downloaded by unsuspecting users. Unauthorized software increases the risk of introducing malicious software to an organisational data and information assets. The goal is to avoid downloading software whose source is unknown. To do this, the following recommendations are suggested:

i. Assigned privileges: The first step to preventing unauthorized software is not to allow such to be installed in the first place. Organisations should clearly designate individuals or teams of IT professionals who will be responsible for downloading, testing, approving, deploying and managing software acquired by organisations. Thus, only approved software can only be downloaded by such people.
ii. Use audit/monitor mode: Depending on the size of an organisation, this could be very strenuous. But most applications offers audit or monitor modes to provide logging and visibility of what software is being executed throughout a user's session. These applications could be used to prevent unauthorised software from getting into an organisation.

5) Not updating work-related passwords regularly

Passwords are known to be most popular means of authentication. However, in recent times, attacking passwords have been one of the most straightforward ventures for hackers. Methods used to compromise passwords range from guessing of passwords to brute attacks. Efforts made to regularly change password could be one measure that can prevent passwords from being compromised. To better manage this CCSB concern, the following suggestions are offered:

(i) Assigned roles: Within an organisation, there should be people whose job it is to update software or passwords.
(ii) Proper password information: Users should be properly educated on how to create strong passwords and to frequently change them.
(iii) Password managers: Organisations should acquire software that is capable of randomly generating passwords for users.

7. CONCLUDING REMARKS

Our study has shed some light on the issue of CCSB commonly practiced by workers based in Nigeria. We succinctly discussed actions that could mitigate the top-five exemplars of CCSB in the context of Nigeria. There are some limitations in our study. First, participants might have provided socially desirable responses to some of the questions we asked in the survey. Second, our data sample is small; a larger sample of sample might offer more useful insights. Third, the data came from a cross-sectional field survey; longitudinal data may offer more robust knowledge. Future study should pay attention to other end user security behaviours, including malicious ones perpetuated by organisational actors. Future studies should carry out comparative studies of findings in developed countries and advanced economies to determine if result compare or differ. Only data provided by mid-level professionals and managers was used for this study. Past studies however showed that the views of top and mid-level managers differ when assessing technologies (Ifinedo and Nahar, 2006). Accordingly, more useful information will surface when the views on CCSB by top and mid-level managers are compared.

8. CONTRIBUTIONS TO KNOWLEDGE

This is one of the few studies of its kind to specifically target the topic of non-malicious, end user security in Nigeria. Our study digresses from the putative issue of cyber-crime that has dominated the literature on IS security in the country. Our study provides nascent information on benign, non-malicious computing practices and acts that can be equally detrimental to the safety of organisational data and informational assets. This area of research has remained largely unexplored in Nigeria. We hoped that this study's focus and contributions will spur on further research and inquiries in the area. Practitioners in Nigeria could use the information provided herein to better manage workers' tendency to participate in CCSB and related IS security malpractice. Importantly, we believe that the foundation of a contingency theory for managing CCSB and related IS security among employees could benefit from insights provided in our study.

REFERENCES

1. Alese, K. A., Thompson, A. F., Owa, K. V., Iyare, O. and Adebayo, O. T. (2014). Analysing issues of cyber threats in Nigeria. Proceedings of the World Congress on Engineering 2014 Vol I, WCE 2014, July 2 - 4, 2014, London, U.K.
2. Bagchi, K., Kirs, P., and Cerveny, R. (2006). Global software piracy: can economic factors alone explain the trend? CACM. 49, 6, 70-75.
3. Bulgurcu, B. H., Cavusoglu, I., and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34, 3, 523-548.
4. Comin, D., and Hobijn, B. (2010). An exploration of technology diffusion. Amer. Econ. Rev. 100, 5, 2031-2059.
5. Conner, C. (2012). Employees Really Do Waste Time at Work. https://www.forbes.com/sites/cherylsnappconner/2012/07/17/employees-really-do-waste-time-at-work/#5f8fb9155e6d
6. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville R. (2013). Future directions for behavioral information security research. Compt. & Sec. 32, 1, 90-101.
7. D'Arcy, J. P. and Devaraj, S. (2012). Employee misuse of information technology resources: testing a contemporary deterrence model. Decision Sci. 43, 6. 1091-1124.
8. D'Arcy, J., Hovav, A., and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inform Syst Res. 20, 1, 79-98.
9. Davenport, T. H. and Short, J. E. (1990). The new industrial engineering: Information technology and business process redesign. MIT Sloan Mgt. Rev. 31, 4, 11-27.
10. Gregorio, D. D., Kassicieh, S. K., and Neto, R. D. (2005). Drivers of e-business activity in developed and emerging markets. IEEE Trans. on Eng. Mgt. 52, 2, 155-166.
11. Guo, K. H., Yufei, Y., Archer, N. P., and Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. J Manage Inform Syst. 28, 2, 203–236.
12. Hu, Q., West, R., and Smarandescu, L. (2015). The role of self-control in information security violations: insights from a cognitive neuroscience perspective. J Manage Inform Syst. 31, 4, 6-48.
13. Ibikunle, F., and Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International Journal of cognitive research in science, engineering and education, 1, 1.
14. Ifinedo, P. (2006). Key information systems management issues in Estonia for the 2000s and a comparative analysis. Journal of Global Information Technology Management. 9, 2, 22-44.
15. Ifinedo, P., and Nahar, N. (2006). Do top-and mid-level managers view enterprise resource planning (ERP) systems success measures differently? International Journal of Management and Enterprise Development, 3, 6, 618-635.
16. Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions: is national culture a differentiator? Information Management & Computer Security, 17, 5, 372-387.
17. Ifinedo, P. (2014). Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51, 1, 69-79.
18. Ifinedo, P., and Akinnuwesi, B. A. (2014). Employees' non-malicious, counterproductive computer security behaviors (ccsb) in nigeria and canada: an empirical and comparative analysis. Proceedings of the 6th IEEE International Conference on Adaptive Science & Technology (ICAST), October 29 -31, 2014, Otta, Nigeria.
19. Kamoun F., and Nicho, M. (2014). Multiple case study approach to identify aggravating variables of insider threats in information systems. Communications of the Association for Information Systems, 35, 18, Available at: http://aisel.aisnet.org/cais/vol35/iss1/18.
20. Leonard, L. N. K., and Cronan, T. P. (2001). Illegal, inappropriate, and unethical behavior in an information technology context: a study to explain influences. J Assoc Inf Syst. 1, 1, Article 12.
21. Loch, K. D., Carr, H. H., and Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. MIS Quarterly. 16, 2, 173-186.
22. Longe, O. B, and Chiemeke, S. (2008).Cyber crime and criminality in Nigeria – what roles are internet access points in playing? European Journal Of Social Sciences, 6, 4.

23. Ng, B-Y., Kankanhalli, A. and Xu, Y.C. (2009). Studying users' computer security behavior: a health belief perspective. Decision Support Systems, 46, 4, 815-825.
24. Oyelere, S. and Oyelere, L., (2015). Users perception of the effects of viruses on computer systems - an empirical research. African journal of computing & ICT, 8, 11, 121 - 130
25. Posey, C., Roberts, C. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. (2013). Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Quart. 37, 4, 1189-1210.
26. Stanton, J. M., Stam, K. R., Mastrangelo P., and Jolton, J. (2005). Analysis of end user security behaviors, Computers & Security, 24, 2, 124-133.
27. Vance, A. Siponen, M. and Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. Inform. & Mgt. 49, 190-198.