Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2015 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2015

Effects of Organizational Citizenship Behavior and Social Cognitive Factors on Employees' Non-Malicious Counterproductive Computer Security Behaviors: An Empirical Analysis

Princely Ifinedo
Cape Breton University, princely_ifinedol@cbu.ca

P20. Effects of Organizational Citizenship Behavior and Social Cognitive Factors on Employees' Non-Malicious Counterproductive Computer Security Behaviors: An Empirical Analysis

Princely Ifinedo
Cape Breton University,
princely_ifinedol@cbu.ca; pifinedo@gmail.com

Abstract

Employees' non-malicious counterproductive computer security behaviors (CCSB) at work could put organizations' information-related assets at risk, if unchecked. Using concepts from the social cognitive and organizational citizenship behavior (OCB) theoretical frameworks, this study examined the effects of observational learning/modeling, social support, and OCB (i.e., helping behaviors and civic virtue) on employees' desire to indulge in CCSB. A research model including the aforementioned factors was proposed and tested using the partial least squares (PLS) technique. A survey of Canadian professionals' opinions was used. The result did not affirm the relationship between employees' observational learning/modeling and intentions to engage in CCSB. The results, however, confirmed that social support and OCB (i.e., helping behaviors and civic virtue) have significant negative effects on intentions to engage in CCSB, which, in turn, has a significant positive effect on employees' self-reported indulgence of CCSB at work.

Keywords

Information Security, Organizational Citizenship Behavior, Social Cognitive Theory, Non-Malicious, Counterproductive Computer Security Behaviors, Employees, PLS, and Survey.

1. Introduction

In this digital era, computer-related information security issues and their management have become a source of major concern for organizations of all sizes, all over the world (Richardson 2012; Ifinedo et al. 2014). Threats to organizations' information-related assets can come from both internal and external sources (Loch et al. 1992; Verizon Business Systems 2011; Richardson 2012). In fact, one industry report indicated that 48% of data breaches were attributable to organizational insiders, i.e., employees (Verizon Business Systems 2011). This is because employees have more privileged access to their organization's digital resources than do outsiders. Equally disastrous to organizations' objectives are benign computer-related security practices or acts that employees choose to engage in. For example, employees who respond to spam emails and/or visit unsanctioned Web sites at work inadvertently open back doors for attacks on their organizations' information-related assets. Thus, the human agent, i.e., "the insider," plays a significant role in ensuring whether organizations' information-related assets are safeguarded or not (Richardson 2012; Ifinedo 2012; D'Arcy & Devaraj 2012; Ifinedo 2014b).

Prior BIS research studied computer abuse, misuse, compliance, and noncompliance with IS security procedures in organizations (Herath & Rao 2009a, 2009b; Guo et al. 2011; Ifinedo 2012; D'Arcy & Devaraj 2012; Ifinedo, 2014a; D'Arcy et al. 2014). It is worth noting that lumping together such diverse issues may becloud the understanding of the sorts of factors that may or may not impact each concern. For instance, Guo (2013) argued that factors that explain employees' computer abuse may not necessarily be pertinent to explaining the desire to flout organizations' IS security guidelines. Similarly, the nature of employees' information security acts could either be malicious (i.e., computer fraud and data theft) or non-malicious (i.e., leaving passwords on office desks and using weak passwords). To add to the literature in the area, this study will focus on employees' non-malicious counterproductive computer security behaviors (CCSB). Herein, CCSB draws from the term "counterproductive work behavior" (CWB) in human resource management and psychology literature (Spector & Fox 2010), which refers to employee behaviors that go against the legitimate interests of an organization. CWB is an active and volitional act engaged in by individuals, as opposed to accidental or unintentional actions (Spector & Fox 2010). Accordingly, CCSB refers to employees' computer use practices and general information security behaviors that go against the legitimate interests of an organization. Examples of CCSB considered in this study include visiting non-related Web sites at work, not updating work-related passwords regularly, and so forth. Malicious (harmful) behaviors will not be considered.

The majority of previous BIS research has employed a select few social psychology and criminological theories to explicate information security behaviors in the workplace. However, recent studies (Albrechtsen 2007; Rhee et al. 2009; Moody & Siponen 2013; Guo 2013; Ifinedo 2014a; D'Arcy et al. 2014) have shown that individual dispositions, cognitive and social influences in the work environment greatly impact employees' IS security behaviors. Research into the effects of such factors has not received extensive recognition in BIS. To add to the literature, this study will investigate the effects of prosocial behaviors and social cognitive influences on employees' desire to indulge in CSSB in the workplace. To that end, this study is the first of its kind to examine the impacts of the aforementioned factors on employees' urge to engage in CCSB. Specifically, the research question posed in this study is: *What effects do organizational citizenship behavior and social cognitive factors have on employees' desire to engage in CCSB*? Accordingly, this study draws from the social cognitive theory (SCT) (Bandura 1986) and organizational citizenship behavior theory (Organ 1988).

2. Background information

2.1 Employees' non-malicious counterproductive computer security behaviors

Various taxonomies on individual IS or information technology (IT) security behaviors have been suggested in the IS security management literature (Loch et al. 1992; Stanton et al. 2005; Guo 2013). This study builds upon the work of Loch et al. (1992), who identified sources of information security threats to an organization; and Stanton et al. (2005), who proposed a taxonomy of end-user computer security behaviors. Regarding the sources of threats, this study focuses solely on human sources, i.e., employees, ex-employees, consultants, and so on. 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. The targets of this current study are employees. Stanton et al. (2005) 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 a trade secret; non-malicious end-user security behaviors include items such as choosing a weak password and responding to spam email. Following a literature search on non-malicious security behaviors and experts' opinions, a list of CCSB was drawn up (Table 1). Other studies in BIS (Stanton et al. 2005; Guo et al. 2011; Chu & Chau 2014) have considered similar items.

2.2 Theoretical background

2.2.1 Social cognitive theory

Social cognitive theory (SCT) posits that individuals acquire and maintain behaviors by emphasizing external and internal social reinforcement (Bandura 1986). It evolved from social learning theory, which asserts that people learn not only from their own experiences but also by observing the actions of others in their environment. Social support and other items have been incorporated into SCT (Bandura 2004). Admittedly, only factors from SCT, which are deemed relevant to this study are considered, i.e., observational learning/modeling and social support. Another major component of SCT, i.e. self-efficacy has already been studied in the context of CCSB (Ifinedo et al. 2014; Ifinedo 2014b). Observational learning/modeling refers to the learning that occurs through observing the behavior of others (Bandura, 1986; 2004). A social model, e.g., co-worker/supervisor, is important in observational learning; such a person facilitates cognitive process behavior of others. Social support refers to the perceived support received from others, i.e., coworkers and supervisors at work (Sarason et al. 1983; Bandura 2004); it enables an individual to interpret events around him or her, guide future behavioral engagements, and enhances the ability to problem-solve (Tilden & Weinert 1987).

2.2.2 Organizational citizenship behavior

Organizational citizenship behavior (OCB) is defined as an individual behavior that promotes the effective functioning of the organization (Organ 1988). OCB exerts positive influence on organizational effectiveness, as it provides socio-emotional support to employees, and facilitates the work of others (Organ 1988; Yen et al. 2008). The construct of OCB is multidimensional (Organ 1988; Podsakoff et al. 2000). Podsakoff et al.'s (2000) dimensions of OCB included helping behavior, civic virtue, loyalty, and so forth. For illustrative purposes, this study employs two dimensions of OCB, i.e., civic virtue and helping behavior, which a study found to be pertinent to IS success in organizations (Yen et al. 2008). Other OCB items are not considered in this study because their potential links with IS variables have not been widely ascertained. That said, civic virtue refers to the willingness of an employee to actively participate in organizational governance and monitor the environment for possible threats, at a personal cost (Podsakoff et al. 2000; Yen et al. 2008). Helping behavior refers to an employee voluntarily helping other employees and preventing work-related problems (Organ 1988; Podsakoff et al. 2000).

3. Research model and hypotheses

The study's research model is shown in Figure 1. It includes control variables, such as age, years of IT use, and IT knowledge to determine their effects on the dependent variable. Past studies have shown that such variables are related to employees' perceptions of computer security issues (e.g., D'Arcy & Devaraj 2012).

It is possible that where employees go above and beyond job requirements to help colleagues identify potential threats to organizational effectiveness, the urge among workers to indulge in

such behaviors will be at a minimum. If such assistance is readily available, for example, to the less knowledgeable, this could sensitize them to the dangers of unsanctioned norms and practices to organizational functioning and success. Workers' helping behavior and civic virtue have been shown to positively impact organizational performance and efficiency (Walz & Niehoff 2000). Logically, the absence of such will lead to organizational inefficiency. With regard to CCSB, helping behavior was shown to have a negative correlation with misuse of IS resources (Chu & Chau 2014). Therefore, it is hypothesized that:

H1*: Organizational citizenship behavior (as indicated by helping behavior and civic virtue) will have a negative effect on intention to engage in CCSB.*

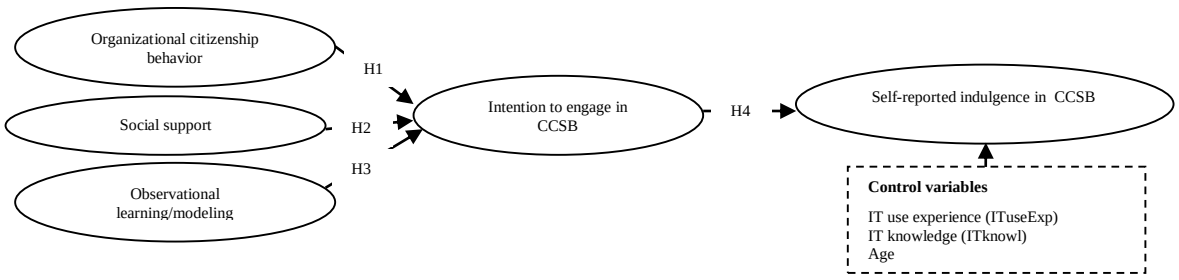

Figure 1: The Research Model

Social support received from the supervisor and colleagues is critically important in shaping the behaviors of workers in an organization (Sarason et al. 1983). Current and future behavioral engagements, as well as the ability to solve problems related to a target behavior, are positively impacted where such support is available (Tilden & Weinert 1987; Glomb & Liao 2003). If employees can rely on and receive needed support from colleagues related to avoiding CCSB, it is likely that the urge to engage in such behaviors will diminish (Herath & Rao 2009b; Bulgurcu et al. 2010). Conversely, the lack of coworker support in such matters can result in an individual's urge to commit unacceptable, antisocial acts or engage in negative behaviors (Glomb & Liao 2003). Thus, where social support is high, the urge to engage in CCSB will be low. Therefore, it is hypothesized that:

H2*: Social support will have a negative effect on intention to engage in CCSB.*

According to SCT (Bandura 1986), people can expand their outcomes on the basis of information conveyed through the observation of others. In the context of computer software training, Yi and Davis (2003) found that observational learning processes significantly influenced training outcomes. Previous research suggested that group perceptions and observation of significant others mattered in employees' desire to comply with their organizations' IS rules and procedures (Bulgurcu et al. 2010; Guo et al. 2011; Ifinedo, 2014a). Thus, it is logical to expect that, with respect to acceptable computing behaviors, workers who have successfully learned and modeled coworkers and supervisors in such matters would shun CCSB, and those who have not may continue to engage in such behaviors. Therefore, it is hypothesized that:

H3*: Observational learning/modeling of coworkers/supervisors who sanction will have a negative effect on intention to engage in CCSB.*

Sheppard et al. (1988) and others in examining the link between intention to engage in a specific behavior and actual behavior showed that intentions are strong predictors of behaviors. In the BIS literature, Moody and Siponen (2013) showed that intention to comply with information security policies has a significant effect on actual compliance with such policies. In general, the relationship between intentions and behavior has been shown to be consistently strong across contexts (Sheeran 2002). That noted, it is hypothesized that:

H4*: Intention to engage in CCSB will have a positive effect on self-reported indulgence in CCSB.*

3. Research methodology

Pre-test and pilot surveys were conducted to enhance the content and face validities of the items used (Ifinedo et al. 2014). The final survey was administered through Fluidsurvey.com. Canadian professionals with knowledge of CCSB were contacted. Data of 201 respondents was used in the final sample. 35% of participants were female, and 65% were males. 38% and 27% of them were in the 30 to 40 and 41 to 50 age range, respectively. Over 90% of them have university education. The average years of computer use was 19.2 years (S.D. = 6.2) and have 6.7 years (S.D. = 6.0) tenure at their current organizations. Some of the participants' job titles include financial manager, engineer, business analyst, IT consultant, and senior accountant. Diverse industries such as energy, services, IT, manufacturing, healthcare, and so forth were included in the sample. The data sample include an evenly distribution of organization size and annual revenue. 48 respondents came from organizations with 251 to 500 employees and 36 participants are from organizations with 5000 workers and above. The majority of the participating organizations' annual revenue is between $1and $9.9 million (18%). 16% and 6% of them have revenues between $10 and $99 million and $ 1 billion and above, respectively. As the survey method used collected both independent and dependent data from the same source, common method variance (CMV) cannot be ruled out. CMV refers to a bias in the dataset due to something external to the measures used in the study. Procedural remedies recommended by Podsakoff et al. (2003) in reducing the effects of CMV were followed.

3.1 The study's constructs

The items used to assess CCSB (Table 1) were sourced from the extant BIS literature and experts; full discussion on the items' development and validation will be provided elsewhere in the literature. Participants in this study were asked the question: "Please indicate how often you indulge in the CCSB listed in Table 1." Their responses were assessed on a seven-point Likert scale ranging from "Almost never" (1) to "Almost always" (7).

Four measures from Yi and Davis (2003) were used to operationalize the observational learning/modeling construct. Two measures were used to represent social support; these were borrowed from Sarason et al. (1983). Intention to engage in CCSB was measured using a three-item scale adapted from Bulgurcu et al. (2010) and Ifinedo (2014a). Given the multidimensional nature of organizational citizenship behavior, this factor was represented as a second-order factor with first-order factors, i.e., helping behavior and civic virtue. Two measures borrowed from Podsakoff et al. (1997) and Yen et al. (2008) were used to assess helping behavior and civic virtue. All the independent variables were assessed on a seven-point Likert scale ranging from "Strongly disagree" (1) to "Strongly agree" (7). The description of the study's measures, their descriptive statistics, and their standardized factor loadings are shown in Table 2.

No.	CCSB Item	p values	VIF
#1	Allowing one's family (i.e. children) to play with work laptop	<0.001	1.372
#2	Not updating anti-virus and/or anti-spyware software at work	0.044	1.123
#3	Using weak passwords at work	0.007	1.227
#4	Not updating work-related passwords regularly	0.086+	1.658
#5	Visiting non-related websites at work	0.038	1.168
#6	Pasting or sticking computer passwords on office desks	<0.001	1.534
#7	Not backing up data files as frequently as possible	0.093+	1.620
#8	Responding to spam (i.e. unsolicited emails)	<0.001	1.372
#9	Downloading unauthorized software (i.e. freeware) onto work computer	0.005	1.342
#10	Not logging out of secure systems after use	0.008	1.124
#11	Disclosing work-related passwords to others	<0.001	1.687
#12	Leaving one's work laptop unattended (i.e. outside work environments)	0.008	1.285
#13	Not always treating sensitive data carefully	<0.001	1.394

Table 1: The List of CCSB Considered in the Study

Construct (Second-order)	First-order factor	Measuring item	Standardized factor loading
	Social support (Socsup) (Mean =4.17; SD= 1.68)	I can count on my coworkers/supervisors to help me avoid CCSB.	0.943
		I can talk about CCSB and related problems with my coworkers/supervisors.	0.947
	Observational learning/modeling (Obsverm) (Mean =4.11; SD= 1.52)	I pay attention to coworkers'/supervisors' computer security behaviors and practices.	0.788
		I have opportunity to process computer security behaviors/practices demonstrated by coworkers/supervisors.	0.798
		I have opportunity to accurately reproduce computer security behaviors/practices demonstrated by coworkers/supervisors.	0.909
		I am motivated by coworkers'/supervisors' computer security behaviors and practices.	0.875
Organizational citizenship behavior (Orclbv)	Civic virtue (Mean =4.69; SD= 1.36)	I actively participate in activities relevant to protecting my organization's data and information.	0.904
		I take the initiative to call attention to any problems with my organization's information security.	0.900
	Helping behavior (Mean =4.40; SD= 1.44)	I go out of my way to help colleagues understand problems related to CCSB.	0.906
		I voluntarily help colleagues prevent the occurrence of problems related to CCSB.	0.904
	Intention to engage in CCSB (Intent) (Mean =4.96; SD= 1.36)	It is possible that I will engage in some form of CCSB, in the future.	0.926
		I am certain that I will engage in some form of CCSB, in the future.	0.939
		I am likely to engage in some form of CCSB, in the future.	0.946

Table 2: The Questionnaire's Items and Descriptive Statistics, and Standardized factor loading

4. Data analysis

The partial least squares (PLS) technique was used for data analysis, as it does not require large sample size, and because it supports both formative and reflective models (Chin 1998). This study used WarpPLS 4.0 software to conduct PLS analysis; this software supports both linear and

nonlinear relationships in an integrative manner (Kock 2014). PLS recognizes two components of a casual model: the measurement and the structural models.

4.1 The measurement model

For the reflective constructs, internal consistency and convergent and discriminant validities were carried out to test the psychometric properties of the measures used to represent them (Fornell & Larcker 1981; Chin 1998). Two tests used to evaluate internal consistency of measures are composite reliability (COM) and Cronbach's alpha (CRA) values. Generally, values no less than 0.70 are considered adequate for assessing internal consistency of variables (Chin 1998). Convergent and discriminant validities are assessed by the following criteria: (a) the standardized item loadings should exceed 0.707; (b) the square root of 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); (c) the items should load more strongly on their respective constructs than on other constructs; and (d) the square root of AVE should be larger than the correlations between that construct and all other constructs (Chin 1998). Cross-loadings are obtained by correlating constructs' factor scores with standardized item scores (Kock 2014); the results, in this regard, show that items load more strongly on their respective constructs (omitted here due to space considerations). Table 2 shows that CRA and COM are consistently above the threshold value of 0.70, the AVE ranged from 0.712 to 0.897, and in no case was any correlation between the constructs greater than the squared root of AVE (the principal diagonal element). Overall, the psychometric properties of the measures used for the reflective construct were adequate.

For the formative construct, i.e., CCSB (the dependent variable), the examination of weights in the principal component analysis is suggested (Petter et al. 2007). Another technique for assessing measures used in formative constructs is to test multicollinearity among indicators; excessive collinearity within scales can destabilize the model (Petter et al. 2007). First, the results showed that item weights have significant values. Two CCSB items with insignificant weights were excluded in the analysis. The variance inflation factor (VIF) indicators (Table 1) ranged from 1.123 to 1.687, which are below the recommended 3.3 threshold (Petter et al. 2007), as well as the more stringent value of 2.5 suggested by Kock (2014). *In toto*, convergent and discriminant validities of measures used to represent the formative construct have been assured.

	COM	CRA	AVE	Intent	Selfccsb	Orclbv	Socsup	Obsverm
Intent	0.956	0.931	0.878	**0.937**	0.152	-0.213	-0.192	-0.167
Selfccsb	NA	NA	NA	0.152	NA	-0.046	0.005	0.087
Orclbv	0.902	0.781	0.821	-0.213	-0.046	**0.906**	0.486	0.596
Socsup	0.946	0.885	0.897	-0.192	0.005	0.486	**0.947**	0.464
Obsverm	0.908	0.864	0.712	-0.167	0.087	0.596	0.464	**0.844**

Note: a) Not applicable (NA), Composite reliability (COM), Cronbach's alpha (CRA), Average valance extracted (AVE);
b) Off-diagonal elements are correlations among constructs; c) The bold fonts in the leading diagonals are the square root of AVEs.

Table 3: Composite Reliability, Cronbach Alphas, Aves, and Inter-Construct Correlations

4.2 The structural model

The WarpPLS 4.0 software provides information about the path significance, coefficients, i.e., beta (β), and the coefficient of determination (R^2) for the structural model (Figure 2). With regard to the R^2, all independent variables explained 8% of the variance in intention to engage in CCSB.

Intention to engage in CCSB and the control variables explained 15% of the variance in self-reported indulgence in CCSB.

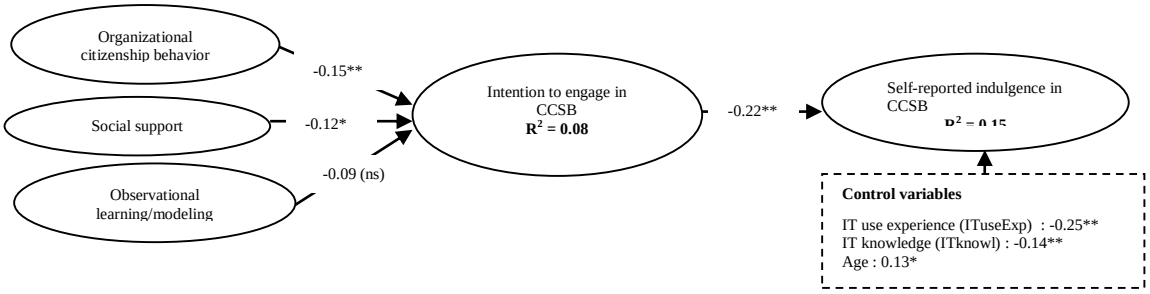

Figure 1: The WarpPLS 4.0 Software's Results

Three out of the four hypotheses were significantly supported. Namely, H1 was confirmed to show that organizational citizenship behavior has a negative effect on intention to engage in CCSB ($\beta = -0.15$, $p < 0.01$). H2, which predicted that social support would have a negative effect on intention to engage in CCSB ($\beta = -0.12$, $p < 0.05$), was confirmed. The relationship between observational learning/modeling and intention to engage in CCSB was unsupported by the data to reject H3 ($\beta = -0.09$, $p = 0.06$). Intention to engage in CCSB has a positive effect on self-reported indulgence in CCSB to significantly uphold H4 ($\beta = 0.22$, $p < 0.01$). Computer skills (IT knowledge), IT use experience, and age were found to have significant effects on self-reported indulgence of CCSB.

5. Discussions and conclusion

The objective of this study was to examine the effects of individual's dispositions in organizational contexts and the influences of social cognitive factors on employees' CCSB. The results show that OCB, as indicated by helping behavior and civic virtue, has a significant negative effect on employees' intention to engage in CCSB. That is, an employee who has more cognitive abilities to actively participate in activities relevant to protecting the organization's data assets, calls the attention of others to such issues, and goes out of his or her way to help colleagues understand and prevent CCSB problems, is less likely to engage in CCSB. This result is consistent with views suggesting that helping behaviors and civic virtues can improve organizational effectiveness and performance (Walz & Niehoff 2000; Yen et al. 2008; Chu & Chau 2014). Social support obtained from supervisors and colleagues serves to discourage a desire to engage in CCSB at work. Employees who can count on their coworkers and supervisors to help them shun CCSB have a greater tendency to avoid CCSB. The reliance on peers' support in understanding CCSB and related problems matters significantly in ensuring that acceptable behaviors related to organizational computer/IS practices are accepted or assimilated (Albrechtsen 2007; Rhee et al. 2009; D'Arcy et al. 2014). This result also mirrors insights that implied group approval of safe and acceptable computing behaviors augurs well for compliance with the sanctioned organization's IS procedures and rules (Bulgurcu et al. 2010; Ifinedo 2014a).

The data analysis did not support the prediction indicating that employees can shun CCSB by observing and modeling computer security behaviors and practices demonstrated by coworkers and supervisors. A plausible explanation for the lack of support for this hypothesis might be due to extraneous influences. For example, it might be possible that this study's participants work in

settings where there are no clear social models for CCSB and related issues. Previous studies (Ifinedo et al. 2014; Ifinedo 2014b) that examined the relationship between observational learning/modeling of coworkers'/supervisors' computer security behaviors and engagements in CCSB showed that two constructs are statistically unrelated. With respect to employees' intentions to engage in CCSB, the result strongly affirms the view indicating that workers with willingness to engage in CCSB go on to commit such a behavior. By the same token, employees with no intentions to indulge in such unsanctioned computer security behavior will avoid CCSB. Congruent to the findings in past BIS studies (Moody & Siponen 2013), this study also provided support for the view suggesting that, *ceteris paribus*, individuals with intentions to comply with their prescribed organizations' IS security policies and guidelines will actually adhere to such. Regarding the control variables, data analysis confirms that the demographic variable of age and individual characteristics related to IT knowledge and IT use experience have impacts on employees' self-reported engagements in CCSB. This study has made theoretical contributions and it is hoped that practitioners derive some benefits from it as well.

5.1 Theoretical contributions

This study is the first of its kind to examine employees' intention to engage in CCSB by using perspectives of individual dispositions (i.e. helping behavior and civic virtue) and social cognitive factors. In particular, no previous study has studied the effects of OCB and social support on intention to engage in CCSB. This study reduces the lacuna in our understanding of factors influencing employees' desire to engage in CCSB and related information security behaviors. This study has shown that other factors, including those with social and cognitive undertones, matter in the discourse. This study is one of the first to link CCSB to CWB in the IS domain. Given that IS-related counterproductive behaviors scarcely get a mention in the literature (Weatherbee 2010; Chu & Chau 2014), its contribution in this regard is welcome. This research effort clearly makes a case for correctly categorizing employees' information security behaviors. It maintains that the nature of employees' information security behaviors should be viewed from the perspective of malicious (i.e., computer fraud and data theft) or non-malicious (i.e., leaving passwords on office desks and using weak passwords). Both should not be treated as being the same. The attention of other researchers being directed to such a distinction could further enhance knowledge in the area. Refinements of this sort benefit BIS research in general.

5.2 Practical implications

To discourage or control employees' desire to engage in CCSB and similar unsanctioned behaviors at work, management should proactively encourage interpersonal, cooperative, and extra-role behaviors among workers in matters related to acceptable computer and IS practices. If it is not possible to instill such qualities into all employees, management should endeavor to identify persons with such nature in the organization, and direct them to be in the vanguard of promoting acceptable and sanctioned practices related to IS and computer use in the organization. Given the critical importance of social support in reducing employees' intention to engage in CCSB, managers and top management should ensure that support and other resources, i.e., the help desk, are made readily available in the organization to anyone who seeks assistance in safe computing and information security practices. When implementing policies and procedures to tackle CCSB, management needs to be aware that variables of age, IT knowledge, and IT use experience, have impacts on employees' indulgence in such behaviors. Namely, older workers and those with greater IT knowledge and use experience are more likely to engage in CCSB at work. Special

attention could be paid to such cohorts of workers in attempt to effectively manage employees' engagements in CCSB and similar unsanctioned computer security practices and behaviors in work settings.

5.3 Study's limitations and future research directions

First, the number of measures used to represent some of the constructs could be increased. Second, as the study used the views of employees, it is difficult to know whether the findings are generalizable to all human agents, i.e., consultants, partners' workers, and ex-employees. Third, the data came from a cross-sectional field survey; longitudinal data may facilitate more insight. Future studies should endeavor to overcome the shortcomings in this study. Attention should be paid to other end-user security behaviors, such as malicious CCSB, in future studies. Other aspects of SCT, i.e., outcome expectancies, facilitators, and self-regulation; and OCB, i.e., loyalty and sportsmanship, could be explored.

Acknowledgement

Funding for this study was received from Social Sciences and Humanities Research Council of Canada.

References

Albrechtsen, E. (2007) "A Qualitative Study of Users' View on Information Security", Computer and Security, 26(4), pp. 276-289.

Anderson, C. L. and Agarwal, R. (2010) "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions", MIS Quarterly, 34(3), pp. 613-643.

Bandura, A. (1986) Social Foundations of Thought and Action: A Social Cognitive Theory, Englewood Cliffs, N.J.: Prentice-Hall.

Bandura, A. (2004) "Health Promotion by Social Cognitive Means", Health Education & Behavior, 31(2), pp. 143-164.

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

Chin, W. (1998) "Issues and Opinion on Structural Equation Modeling", MIS Quarterly, 22(1), vii-xvi.

Chu, A. M. Y. and Chau, P.Y.K. (2014) "Development and Validation of Instruments of Information Security Deviant Behavior", Decision Support Systems, 66, pp. 93–101.

D'Arcy, J. P. and Devaraj, S. (2012) "Employee Misuse of Information Technology Resources: Testing A Contemporary Deterrence Model", Decision Sciences, 43(6), pp. 1091-1124.

D'Arcy, J., Herath, T. and Shoss, M. K. (2014) "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective", Journal of Management Information Systems, 31(2), pp. 285–318.

Fornell, C., D.F. Larcker (1981). Evaluating structural equations models with unobservable variables and measurement error, Journal of Marketing Research, 8(1), 39-50.

Glomb T. M. and Liao H. (2003) "Interpersonal Aggression in Work Groups: Social Influences, Reciprocal and Individual Effects", Academy of Management Journal, 46, pp. 486–496.

Guo, K. H. (2013) "Security-related Behavior in Using Information Systems in The Workplace: A Review and Synthesis", Computers & Security, 32, pp. 242-251

Guo, K. H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011) "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model", Journal of Management Information Systems, 28(2), pp. 203–236.

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

Herath, T. and Rao, H. R. (2009b) "Encouraging Information Security Behaviors: Role of Penalties, Pressures and Perceived Effectiveness", Decision Support Systems, 47(2), pp. 154-165.

Ifinedo, P. (2012) "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory", Computer & Security, 31(1), pp. 83-95.

Ifinedo, P. (2014a) "Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition", Information & Management, 51(1), pp. 69-79.

Ifinedo, P. (2014b) "Social Cognitive Determinants of Non-Malicious, Counterproductive Computer Security Behaviors (CCSB): An Empirical Analysis", the 8th Mediterranean Conference on Information Systems - MCIS2014, Sept. 3 – 5, 2014, Verona, Italy.

Ifinedo, P., Cashin, J. and Ojo, O. (2014) "Social-Cognitive Mechanisms and Counterproductive Computer Security Behaviors (CCSB): An Analysis of Links, the 44th. Annual Atlantic Schools of Business (ASB) Conference, Sept 26 - 28, 2014, Halifax, Canada.

Kock, N. (2014). WarpPLS 4.0 user manual. ScriptWarp Systems. https://dl.dropboxusercontent.com/u/95489293/WarpPLS-Pubs/UserManual_v_4_0.pdf

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), pp. 173-186.

Moody, G. D. and Siponen, M. (2013) "Using the Theory of Interpersonal Behavior to Explain Non-Workrelated Personal Use of the Internet at Work", Information & Management, 50, pp. 322–335

Organ, D. W. (1988) Organizational Citizenship behavior: The Good Soldier Syndrome, Lexington, MA: Lexington Books.

Petter, S., Straub, D. and Rai, A. (2007) "Specifying Formative Constructs in Information Systems Research", MIS Quarterly, 31(4), pp. 623–656.

Podsakoff, P. M., MacKenzie, S. B., Paine, J. B. and Bachrach, D. G. (2000) "Organizational Citizenship Behaviors: A Critical Review of the Theoretical and Empirical Literature and Suggestions for Future Research"' Journal of Management, 26(3), pp. 513-563.

Podsakoff, P. M., Ahearne, M., and MacKenzie, S. B. (1997) "Organizational Citizenship Behavior and the Quantity and Quality of Work Group Performance", Journal of Applied Psychology, 82, pp. 262–270.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y. and Podsakoff, N. P. (2003) "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies", Journal of Applied Psychology, 88(5), pp. 879-903.

Rhee, H., Kim, C. and Ryu, Y. (2009) "Self-efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior"' Computer and Security, 28(8), pp. 816-26.

Richardson, R. (2012) "CSI Computer Crime and Security Survey 2010/2011. Computer Security Institute, New York, Http://gocsi.com/survey/.

Sarason, I. G., Levine, H. M., Basham, R. B. and Sarason, B. R. (1983) "Assessing Social Support: The Social Support Questionnaire"', Journal of Personality and Social Psychology, 47, pp. 378-389.

Sheeran P. (2002). Intention-behavior Relations: A Conceptual and Empirical Review in Stroebe, W. and Hewstone, M. (Eds.) European Review of Social Psychology, 12, Chichester: Wiley, pp. 1-30.

Sheppard, B. H., Hartwick, J. and Warshaw, P.R. (1988) "The Theory of Reasoned Action: A Metaanalysis of Past Research with Recommendations for Modifications and Future Research", Journal of Consumer Research, 15, pp. 325–343.

Spector, P. E. and Fox, S. (2010) "Counterproductive Work Behavior and Organisational Citizenship Behavior: Are They Opposite Forms of Active Behavior?", Applied Psychology: An International Review, 59(1), pp. 21–39.

Stanton, J. M., Stam, K. R, Mastrangelo, P. and Jolton, J. (2005) "Analysis of End User Security Behaviors", Computers & Security, 24(2), pp. 124-133.

Tilden, V. P. and Weinert, S. C. (1987) "Social Support and the Chronically Ill Individual", Nursing Clinics of North America, 22 (3), pp. 613–620.

Verizon Business Systems (2011) "2011 Data Breach Investigations Report, Verizon RISK Team Research Report, New York, NY: Verizon Communications.

Walz, S. and Niehoff, B.P. (2000) "Organizational Citizenship Behaviors: Their Relationship to Organizational Effectiveness", Journal of Hospitality & Tourism Research, 24, pp. 108–126.

Weatherbee, T. G. (2010) "Counterproductive Use of Technology at Work: Information & Communications Technologies and Cyberdeviancy", Human Resource Management Review, 20(1), pp. 35–44.

Yen, H. R. Li, E. Y. and Niehoff, B. P. (2008) "Do Organizational Citizenship Behaviors Lead to Information System Success? Testing the Mediation Effects of Integration Climate and Project Management", Information & Management, 45, pp. 394–402.

Yi. M. Y. and Davis, F. D. (2003) “Developing and Validating an Observational Learning Model of Computer Software Training and Skill Acquisition”, Information Systems Research, 14(2), pp. 146-169.