Investigating Employee Engagement in Nonmalicious, End-user Computing and Information Security Deviant Behavior

Completed Research

Princely Ifinedo
Brock University
pifinedo@brocku.ca

Abstract

Nonmalicious, end-user computing and information security deviant behavior (NECISDB) (e.g., pasting or sticking computer passwords on office desks, downloading unauthorized software onto work computer) are a major concern to organizations. This study used Social Cognitive Theory, in particular, a simplified version of its core - the triadic reciprocal determinism - to investigate effects of relevant socio-organizational and personal cognitive factors (e.g., organizational facilitators, observational learning/modeling, and self-efficacy) on employee engagement in NECISDB. Survey data was collected from 411 professionals in two European Union countries. Relevant hypotheses were formulated and tested. Results reveal that self-efficacy and its joint effect with self-regulation have negative effects on NECISDB engagement intentions. Although observational learning/modeling does not influence NECISDB intentions directly, it does have an indirect effect through self-efficacy. Organizational facilitators, e.g., awareness training and its joint effect with observational learning/modeling did not influence NECISDB intentions. Intentions are positively linked to self-reported engagement in NECISDB.

Keywords

Nonmalicious, information systems security deviant behavior, employees, survey, social cognitive theory.

Introduction

Data breaches can be very problematic to organizations (Armerding, 2018) and their origins are attributable to actions of either internal (e.g., employees) or external (e.g., hackers) entities. Regardless of the source, management tends to commit substantial financial resources to deal with such concerns (Ifinedo, 2018). Technological or technical controls, which are often the considered solution have been found to be inadequate in assuring total security and protection to organizations' digital resources and assets. Researchers (e.g., Stanton et al., 2005; Crossler et al., 2013) have argued that an understanding of the actions or behavior of the human agent is a useful strategy to complement implemented technical measures or controls. Indeed, researchers' and practitioners' communities have recognized the role of the "insider" in initiating security breaches (Loch et al., 1992; Stanton et al., 2005; van Vliet, 2018; Ifinedo, 2019). The "insider" can be grouped into two broad categories: malicious and careless. For example, a disgruntled employee who leaks data or damages his or her organizational information systems (IS) is considered a malicious insider and an employee who clicks on a phishing link in an email is a careless insider (van Vliet, 2018). The focus of this study will be on actions of the nonmalicious or careless insider, which can have disastrous consequences to organizations' objectives (Stanton et al., 2005; van Vliet, 2018). While a growing body of academic literature has studied the malicious insider (e.g., Jones, 2008), few researchers have investigated nonmalicious computing and information security deviant behaviors (e.g., Guo et al., 2011). In some instances, nonmalicious and malicious actions have been mixed (e.g., D'Arcy et al., 2009). There is a need to separate both in order to enrich understanding in the area (e.g., Stanton et al., 2005; Ifinedo, 2019).

Thus, this study's dependent construct is in nonmalicious, end-user computing, and information security deviant behavior (NECISDB), which refers to the willful or volitional use of computing technologies and general IS tools in a manner contrary to the legitimate interests and goals of an organization. The focus on NECISDB is beneficial to knowledge, and it departs from efforts discussing generic IS security compliant behavior, which is well-represented in the extant literature (Sommestad et al., 2014). Emphasis on NECISDB ensures a clear understanding of its antecedent factors; accordingly, appropriate management strategies to deal with the phenomenon can surface.

Comprehensive reviews of behavioral theories most frequently used to explicate IS security compliant behavior include Theory of Reasoned Action/Theory of Planned Behavior (TRA/TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT), Technology Acceptance Model (TAM), Social Learning Theory (SLT), and Social Cognitive Theory (SCT) (Sommestad et al., 2014; Ifinedo, 2018). Among the least used theoretical frameworks from the list is SCT, which incidentally is employed to guide this current research study. SCT was chosen because researchers (e.g., Warkentin et al., 2011; Guo et al., 2011; Willison and Warkentin, 2013) have argued that the interplay between the environment (i.e., organization, social interaction in work settings) and individual cognitive beliefs (e.g., self-efficacy) plays a critical role in understanding employees' IS security deviant behaviors. It is not suggested herein that the other theories matter less; rather, this study maintains that an underexplored theory such as SCT could offer useful insights to complement or extend perspectives in prior studies that used other relevant theoretical frameworks. Moreover, SCT is suitable for studies investigating the impacts of socio-organizational and personal cognitive factors on a behavior, which is this study's focus.

The constructs of SCT of pertinence to this study include organizational facilitators, observational learning/modeling, self-efficacy, self-regulation, and intention. Previous research has shown that organizational facilitators such training and security awareness programs (e.g., D'Arcy et al., 2009), observational learning/modeling (e.g., Warkentin et al., 2011; Guo et al., 2011), self-efficacy (e.g., Ifinedo, 2014), and self-regulation (e.g., Hu et al., 2011) influence employee intention to adhere to IS security compliant behavior. To contribute to the knowledge of factors influencing employee engagement in NECISDB, this study explores the direct effects of observational learning/modeling and self-efficacy on intention to engage in NECISDB, and ultimately on self-reported participation in the behavior. Accepting that rarely do independent factors, such as observational learning/modeling and self-efficacy, act in isolation to influence a behavioral outcome for an end-user, the interacting or moderating effects of organizational facilitators and self-regulation were included in the proposed research model to enrich insight (please see Chen et al. (2012) for more information on interacting effects in IS security studies). Not many researchers have examined the interacting effects of variables in the context of IS security. The study that did, indicated that deeper knowledge ensued from such an exercise (Chen et al., 2012).

Following the preceding discussions, the research questions posed in this study are presented as follows:

Q1: What effects do social-organizational (i.e., observational learning/modeling) and personal cognitive (i.e., self-efficacy) factors have on employee engagement in NECISDB?

Q2: What are the moderating effects of organizational facilitators and self-regulation in the relationships between the aforementioned factors and employee engagement in NECISDB?

Background Information

Research on NECISDB is just emerging. In fact, Guo and colleagues (Guo et al, 2011; Guo and Yuan, 2012) were among the first IS security researchers to pay specific attention to the phenomenon. Guo e al. (2011) demonstrated that attitude and personal beliefs, among others, affected individuals' willingness to engage in NECISDB. Others (e.g., Chu and Chau, 2014; Ifinedo, 2019) have attempted to identify and categorize employees' nonmalicious IS security risk behaviors. It is worth noting that sub-components of NECISDB have also been used in other studies. For example, the scenario items used in Guo and Yuan (2012) to study employee violations of IS security rules are indeed NECISDB items. Moody and Siponen (2013) used an NECISDB item, i.e., non-work-related personal internet use at work in their study; they found that employees' habits, personal beliefs, and attitudes are strong impetuses. Previous research has not investigated the impact of the selected variables in this study on NECISDB to underscore the relevance of this present endeavor. That noted, this study draws from Loch et al. (1992) who identified sources of information security threats to an organization. To that end, the source of IS security threats considered in this study is the human agent, i.e., employees. Stanton et al. (2005) offers a taxonomy of end-user security risk behaviors and categorizes the nature or acts as either malicious or nonmalicious. As already indicated, the emphasis of this study is on the latter. Following the classifications of nonmalicious end-user security behaviors in the literature (e.g., Chu and Chau, 2014; Ifinedo, 2019), this study uses three categories of NECISDB with examples (Table 1). Namely, the three categories used are “careless use of IS resources”, “procrastinating carrying out required IS actions”, and “improper use of IS resources”.

Theoretical Foundation

Social Cognitive Theory (SCT), which was proposed by Bandura (1986), has been used in several disciplines including management, psychology, education, and so forth. SCT posits that individuals acquire and maintain behaviors by emphasizing internal and external or environmental reinforcements. SCT factors are numerous; only those deemed relevant to this study are considered. At the core of SCT is a model of causation involving triadic reciprocal determinism that highlights reciprocal causation among behavior, personal cognitive factors, and environmental influences (Bandura, 1986). The model is highlighted in Figure 1a to show the interacting determinants of personal factors, behavior, and the environment in a bidirectional fashion. For the purposes of this study, a simplified version of the model will be used as did others (e.g., Griffin, 1997). In fact, Griffin, (1997, p. 760) commented that “there is a frequent tone of pessimism that such an interaction can be captured by anything except the most complex research enterprises.” Thus, the study’s research model (Figure 1b) is expanded to include examples of each factor and only forward casual associations leading to behavior are considered.

Research Model and Hypotheses

The research model with the proposed hypotheses and relevant control variables is shown in (Figure 1b). Evidence suggests that these control variables (e.g., age, gender) impact end-user IS security behavior (e.g., D’Arcy et al., 2009; Ifinedo, 2018). Guidelines from the literature were used to delineate the constructs into reflective (rectangle-shaped) and formative (rounded rectangle-shaped) constructs (Petter et al., 2007). Discussions on the study’s hypotheses are provided as follows:

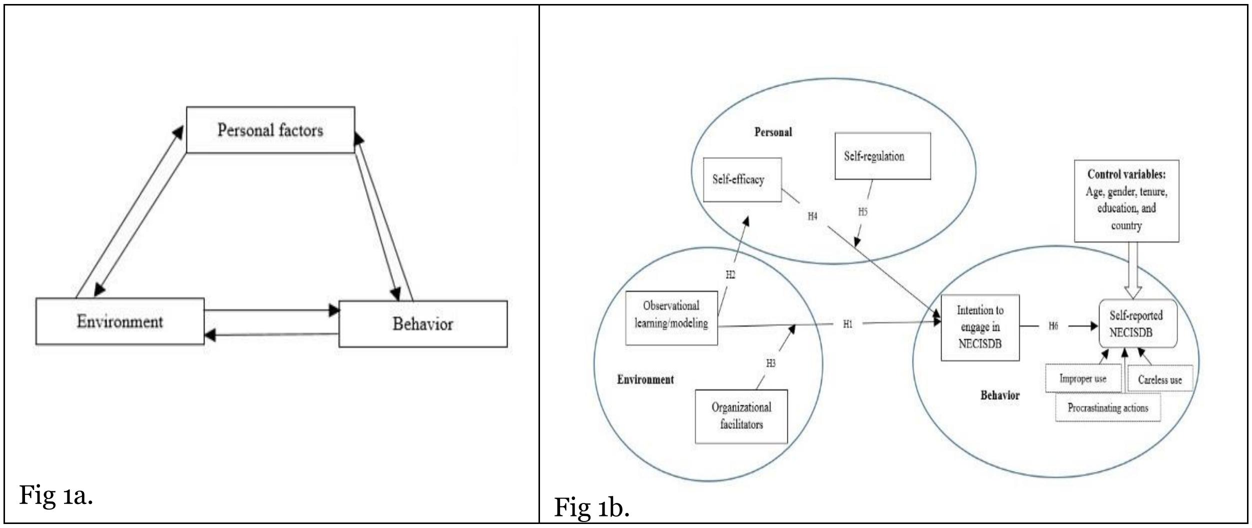

Fig 1a.

Fig 1b.

Figure 1a. Bandura’s Triadic Reciprocal Determinism & Figure 1b. The Research Model

Observational learning/modeling refers to learning that occurs through observing the behavior of others (Bandura, 1986). It is akin to vicarious learning experience, which refers to behavior or skill derived from seeing the performance of others (Bandura, 1986). Observational learning/modeling positively influence successful learning outcomes, especially in day-to-day, informal settings (Warkentin et al., 2011). The behaviors of influential coworkers and supervisors at work are often imitated by other workers (Guo et al., 2011). Accordingly, coworkers’/supervisors’ computer security behaviors and practices may be copied by others. It is expected that workers who have successfully learned and modeled their behaviors after coworkers’ and supervisors’ acceptable computing and IS security practices will have less willingness to participate in NECISDB. Warkentin et al. (2011) showed that observational learning was an important antecedent to information privacy policy compliance. Further, studies have shown that employees' self-efficacy to take appropriate IS security actions is positively influenced by the behavior of others they see around them (e.g., Bulgurcu et al., 2010; Warkentin et al., 2011). Therefore, it is hypothesized that:

H1: Observational learning/modeling of coworkers'/supervisors' IS security actions will have a negative effect on employee intention to engage in NECISDB.

H2: Observational learning/modeling of coworkers'/supervisors' IS security actions will have a positive effect on employee self-efficacy with regard to NECISDB.

In this study, organizational facilitators refer to available supportive incentives, e.g., access to training and IS security awareness programs. Past research suggests that workers who have access to IS security training and other awareness programs are less likely to misuse or abuse organizational computing resources (D'Arcy et al., 2009). In contexts where employees learn from other colleagues in the work environment and organizational facilitators such as training are readily available, it is expected that prescribed work activities will thrive. It is predicted that the joint effect of organizational facilitators and observational learning/modeling of coworkers'/supervisors' acceptable IS security practices will diminish intention to participate in NECISDB. Therefore, it is hypothesized that:

H3: The joint effect of organizational facilitators and observational learning/modeling of coworkers'/supervisors' IS security actions will have a negative effect on employee intention to engage in NECISDB.

Bandura (1986) describes self-efficacy as an individual's belief in his or her ability to execute courses of action required to accomplish a task. According to Bandura, self-efficacy plays a major role in determining a person's intentional behavior. Thus, high levels of self-efficacy have been shown to be positively related to high levels of performance or achievement (e.g., Bandura, 1986). Several IS security and privacy researchers have demonstrated that individuals' self-efficacy, with regard to end-user IS security issues, is an important determinant of intention to comply with organization's IS rules and guidelines (Bulgurcu et al., 2010; Warkentin et al., 2011). Thus, it is reasonable to expect that employees' intentions to engage in NECISDB will likely be low if they possess the competency and capabilities to deal with such concerns.

H4: Self-efficacy will have a negative effect on employee intention to engage in NECISDB.

Self-regulation refers to the ability to control one's behavior in the pursuit of long-term goals. It can minimize an individual's tendency to engage in deviant behavior (Bandura, 1991). According to Bandura (1991), the three processes contained in self-regulation are self-observation, self-judgment, and self-response. He noted that individuals with high self-regulation through forethought are able to guide themselves in anticipatory proactive ways. Researchers across disciplines have shown that self-efficacy and self-regulation are positively associated (e.g., Schunk and Zimmerman, 2007). Guo and Yuan (2012) showed that the "self-regulatory approach" of personal self-sanctions has a negative effect on intentions to engage in NECISDB. It is expected that employees' intentions to engage in NECISDB will likely be low with high levels of self-efficacy and self-regulation. Therefore, it is hypothesized that:

H5: The joint effect of self-efficacy and self-regulation will have a negative effect on employee intention to engage in NECISDB.

Intention refers to an indication that an individual is willing or ready to perform a given behavior (Webb and Sheeran, 2006). Meta-analytic evidence indicated that changes in intention lead to actual behavior (Webb and Sheeran, 2006). This study used self-reported engagement in NECISDB in lieu of actual observed engagement (actual behavior). Past studies found self-reported behavior is positively associated with actual behavior (e.g., Corral-Verdugo, 1997). In the IS security literature, studies have shown that intention to comply with information security policies has a significant effect on actual compliance with such policies (Moody and Siponen, 2013). Therefore, it is hypothesized that:

H6: The employee intention to engage in NECISDB will have a positive effect on self-reported NECISDB.

Research Methodology

To validate the research model, the survey method was used. Pre-test and pilot surveys were carried out to enhance the content and face validities of the study's items. The main survey used the services of a data research firm to collect data; others did likewise (e.g., Bulgurcu et al., 2010). This approach helps to circumvent the difficulty in obtaining information-security information from organizations. Participation was voluntary and only full-time, mid-level career employees of organizations were recruited. Data were collected in two European Union countries, i.e., Sweden and Germany where workers' have relatively high levels knowledge of IS security and privacy issues (e.g., Warkentin et al., 2011). The questionnaire was translated into local languages using recommended guidelines. Precisely, 1,899 and 1,008 opted to participate in the survey by accepting the consent agreement in Sweden and Germany, respectively. Excluding incomplete responses and poorly completed responses, the usable data has 411 responses with 204 and 207 Swedish and German sub-samples, respectively.

In the sample, 25.0%, 25.32%, and 24.6% of respondents were in the 21 to 30, 31 to 40, and 41 to 50 age ranges, respectively. The sample's average years of computer use was 18.7 years (standard deviation (S.D.) = 7.0), average tenure at their current places of work was 7.2 years (S.D. = 7.3). Some of the participants' job titles include financial manager, project manager, IT manager, analyst, and accountant. Diverse industries, such as retail, manufacturing, financial services, and healthcare, were included in the sample. The data sample includes an even distribution of organization size and annual revenue. 65 (15.8%), 48 (11.7%), and 57 (13.9%) of the respondents come from organizations with 51-250, 251-500, and 501-1000 employees, respectively. This study addressed the threat of common method bias (CMB), which can arise whenever survey data collects both the independent and dependent variables from the same source (Podsakoff et al., 2003). Recommended precautionary actions and procedures for data collection and instrument designed were followed. Notably, respondent anonymity was assured by the data collection used by this study. Additionally, the assessment of full collinearity variance inflation factors (VIFs) (Kock, 2015) was used to determine if CMB was a problem for the collected dat. The collinearity VIFs for latent variables of self-regulation, organizational facilitators, observational learning/modeling, self-efficacy, intention, and NECISDB are 1.71, 1.40, 1.58, 1.52, 1.30, and 1.16, respectively. These values are below the conservative threshold of 2.5, which is used to indicate the presence of CMB in a model (Kock, 2015).

Study's Constructs

The items used to represent NECISDB and its sub-constructs (Table 1) were sourced from Ifinedo (2019). Participants were asked the question: "Please indicate how often you participate in the NECISDB listed in Table 1." Their responses were assessed on a seven-point Likert scale, ranging from "Almost never" (1) to "Almost always" (7).

NECISDB sub-category	**NECISDB item**	**Mean**	**SD**	**Weight**	**p-value**	**VIF**
Careless use of IS resources	Not always treating sensitive data carefully	2.78	1.93	0.388	<0.001	1.27
	Pasting or sticking computer passwords on office desks	2.44	1.90	0.420	<0.001	1.43
	Disclosing work-related passwords to others	2.18	2.09	0.450	<0.001	1.58
Improper use of IS resources	Visiting non-related websites at work	4.34	2.13	0.338	<0.001	1.21
	Downloading unauthorized software (i.e., freeware) onto work computer	2.71	2.10	0.354	<0.001	1.22
	Not logging out of secure systems after use	3.52	1.81	0.393	<0.001	1.32
Procrastinating carrying out	Not updating work-related passwords regularly	4.15	1.88	0.499	<0.001	1.14

required IS actions	Not updating anti-virus and/or anti-spyware software at work	3.00	1.95	0.550	<0.001	1.19
	Not backing up data files as frequently as possible	3.88	1.67	0.364	<0.001	1.05

Table 1. The NECISDB items, their descriptive statistics, and indicators

Measures of self-efficacy were adapted from Bulgurcu et al. (2010). Items for self-regulation were modified from William et al. (1996). Measuring items used for organizational facilitators were adapted from D'Arcy et al. (2009). Measures used to operationalize the observational learning/modeling construct were taken from Yi and Davis (2003). Measures used to represent intention to engage in NECISDB were obtained from Ifinedo (2014). All the measuring items used for these reflective constructs were assessed on a 7-point Likert scale, ranging from "Strongly disagree" (1) to "Strongly agree" (7). Questionnaire items for the reflective constructs and their descriptive statistics are shown in Table 2.

Construct	**Item description**	**Mean**	**SD**	**Item loading**
Organizational facilitators	My organization provides relevant training on safe computing and acceptable IS security practices.	3.86	1.81	0.912
	My organization provides IS security awareness campaigns/programs to employees.	4.15	1.73	0.919
	My organization provides guidelines that govern what employees are allowed to do with their computers and other digital resources.	4.02	1.53	0.905
Self-regulation	I take it upon myself not to engage in NECISDB.	4.91	1.45	0.818
	I self-monitor my activities to make sure I do not inadvertently engage in NECISDB.	4.88	1.39	0.867
	If I found myself engaging in NECISDB, I would be very upset.	4.52	1.57	0.801
Self-efficacy	I believe I have the knowledge and ability to avoid engaging in NECISDB.	4.93	1.31	0.970
	I find it easy to implement preventative measures against NECISDB.	4.72	1.26	0.856
	I have the skills and expertise to avoid NECISDB.	4.90	1.29	0.900
Observational learning/modeling	I pay attention to co-workers'/supervisors' computer security behaviors and practices.	4.01	1.62	0.817
	I have the opportunity to process computer security behaviors/practices demonstrated by co-workers/supervisors.	4.20	1.48	0.873
	I have the opportunity to accurately reproduce computer security behaviors/practices demonstrated by co-workers/supervisors.	4.05	1.53	0.824
	I am motivated by co-workers'/supervisors' computer security behaviors and practices.	4.00	1.60	0.751
Intention to engage in NECISDB	It is possible that I will engage in some form of NECISDB, in the future.	3.97	1.67	0.927
	I am certain that I will engage in some form of NECISDB, in the future.	3.83	1.70	0.926
	I am likely to engage in some form of NECISDB, in the future.	3.93	1.74	0.946

Table 2. Questionnaire's items (reflective construct), their descriptive statistics and item loadings

Data Analysis

The partial least squares structural equation model (PLS-SEM), which does not require large sample sizes and data normality, was used for data analysis (Hair et al., 2017). WarpPLS 5.0 software was used for analysis. PLS-SEM allows research models to be tested in two stages: the measurement and structural models.

Measurement Model

Item reliability, composite reliability, and convergent and discriminant validities were used to assess the psychometric properties of the reflective models. Loadings above 0.7 are recommended for assessing item reliability (Hair et al., 2017) and two commonly used indicators are composite reliability and Cronbach's alpha. Entries in Table 2 show that the study's item reliability are satisfactory. Convergent and discriminant validities are assessed by the following criteria: (a) standardized item loadings should exceed 0.707; (b) indicators should load much higher on their hypothesized factor than on other factors (i.e., own-loadings are higher than cross-loadings). This condition was met but not included due to space consideration; (c) the average variance extracted (AVE) should be at least 0.5 to show the construct-related variance is higher than error variance (Hair et al., 2017); and (d) the square root of AVE should be larger than the correlations between that construct and all other constructs in the model (Hair et al., 2017). Table 2 shows that all AVEs are above the recommended threshold of 0.50. In no case was any correlation between the constructs greater than the squared root of AVE (the principal diagonal element). The foregoing information indicates that the quality of the study's measurement model is satisfactory. For the formative construct, it is recommended that item weights and the presence of multicollinearity are checked (Petter et al., 2007). Items weights show how significantly linked item indicators are to their specified constructs. Excessive collinearity within formative scales is undesirable as it can make the construct unstable. To assess multicollinearity among the variables, the variance inflation factors (VIF) are checked. VIFs below the conservative cutoff of 3.33 are considered adequate (Petter et al., 2007). WarpPLS 5.0 provides information on VIF and item weights. Table 1 shows that VIFs and item weights used to capture sub-categories of NECISDB are adequate, and all the VIFs are below 3.33. The item weights are all significant at p <0.001 level.

	CRA	COM	AVE	1	2	3	4	5	6
1: Observational learning/modeling	0.83	0.90	0.69	**0.83**	0.3	0.03	0.44	0.40	0.47
2: NECISDB	0.73	0.85	na	0.03	na	0.30	-0.14	-011	-0.02
3: Intention	0.92	0.95	0.87	0.03	0.30	**0.93**	-0.08	-0.24	-0.10
4: Self-efficacy	0.87	0.92	0.79	0.44	-0.14	-0.08	**0.89**	0.48	0.31
5: Self-regulation	0.77	0.87	0.69	0.40	-0.11	-0.24	0.48	**0.83**	0.31
6:Organizational facilitators	0.90	0.94	0.83	0.47	-0.02	-0.10	0.31	0.31	**0.91**

Note: a) COM = composite reliability; CRA = Cronbach's alpha; AVE = average variance extracted; na = applicable; b) Off-diagonal elements are correlations among constructs; c) the bold fonts in the leading diagonals are the square root of AVEs.

Table 2. Composite Reliability, AVEs, and inter-construct correlations

Structural Model

The antecedent factors explained 10% of the variance in intention to engage in NECISDB, which together with the control variables accounted for 14% of the variance in the dependent construct: self-reported NECISDB. The Goodness of Fit (GoF) is a global fit measure that accounts for both measurement and structural model performance (Tenenhaus et al., 2005). The GoF obtained for this study is 0.32, which is close to the cut-off value of 0.36 for large effect sizes (Wetzels et al., 2009). Four (4) out of the six (6) hypotheses formulated were significantly supported. Inconsistent with H1, observational learning/modeling of coworkers'/supervisors' IS security actions was not found to have a negative effect on employee intention to engage in NECISDB ($\beta = 0.05$, $p = 0.16$). Supporting H2, the result shows that observational learning/modeling of coworkers'/supervisors' IS security actions had a positive effect on employee self-efficacy related NECISDB issues ($\beta = 0.44$, $p < 0.01$). The data did not support H3, which predicted that the joint effect of organizational facilitators and observational learning/modeling of coworkers'/supervisors' IS security actions would have a negative effect on employee intention to engage in NECISDB (β = -0.05, p = 0.16). Support was found for H4, which predicted that self-efficacy related to NECISDB would have a negative effect on employee intention to engage in NECISDB (β = -0.07, p < 0.10). The result shows that the joint effect of self-efficacy and self-regulation had a negative effect on employee intention to engage in NECISDB to support H5 (β = -0.13, p < 0.01). The positive effect of intention to engage in NECISDB on self-reported NECISDB was upheld to support H6 (β = 0.29, p < 0.10). The data also showed that younger workers (β = -0.15, p <0.01) and males (β = -0.08, p <0.10) are more likely to participate in NECISDB.

Discussion and Conclusion

The objective of the study was to investigate the effects of social-organizational (i.e., observational learning/modeling, organizational facilitators) and personal cognitive (i.e., self-efficacy, self-regulation) factors on employee engagement in NECISDB. The unsupported hypotheses were discussed first. The data did not indicate that observational learning/modeling of coworkers'/supervisors' IS security actions has a negative effect on employee intention to engage in NECISDB. Two plausible reasons are offered for the lack of this hypothesis: a) it is possible the study' participants work in settings where no noticeable role model behaviors for NECISDB can be observed and copied. Gist (1978) indicated that observational learning is effective when the modeled behavior is clear and visible; b) it is possible that this study's operationalization of observational learning/modeling construct is inadequate. For example, while this study used only 4 items to represent the construct, Yi and Davis (2003) used a lot more items to capture it. The unsupported prediction of the joint effect of organizational facilitators and observational learning/modeling on intention to engage in NECISDB could be attributable to the above-noted research design problem and other extraneous factors. For instance, the mean of the organizational facilitators' items is lower than those of the other antecedent factors to suggest that the study's participants ascribed lower value to the construct. This information suggests that the study's participants might have come from organizations where facilitating conditions are not considered sufficient. This result is somewhat surprising. Other IS security studies (e.g., Pahnila et al., 2007) showed that organizational facilitators did not positively influence compliance intention with IS rules.

The result shows that when employees are able to learn and model IS security practices after colleagues' (i.e., coworkers and supervisors), their individuals' self-efficacy with respect to NECISDB increases. This finding offers support to observations in prior studies (e.g., Warkentin et al., 2011; Guo et al., 2011) that showed employees' self-efficacy to take appropriate IS security actions benefit from observing the practices of others around them. Similarly, employees' self-efficacy with regard to IS security measures augurs well for diminishing intention to engage in NECISDB. This result lends credence to insights in prior studies that demonstrated the significance of individuals' self-efficacy in dealing with end-user IS security issues and resisting the urge to participate in proscribed IS security practice (e.g., Bulgurcu et al., 2010). The joint effect of self-efficacy and self-regulation as a force to discourage employee intention to engage in NECISDB is underscored. That is, employees who simultaneously possess self-regulation and self-efficacy in relation to acceptable IS security practices are better equipped to minimize their tendency to engage in IS security deviant behavior (e.g., Guo and Yuan, 2012), and proactively guide against participation in such behaviors (Bandura, 1991). In general, support is provided to previous studies indicating favorable outcomes ensue from tasks benefitting from self-regulation and self-efficacy (Schunk and Zimmerman, 2007). The data permitted the insight that employees with a willingness to engage in NECISDB go on to participate in the behavior. As a corollary, employees with no intentions to engage in the behavior will avoid or shun it. The result affirms the existence of a positive relationship between intention and actual behavior in general (e.g., Corral-Verdugo, 1997), and in the context of IS security behavior (e.g., Moody and Siponen, 2013).

Contributions to Research and Implications for Practice

The results of the study show that SCT is suitable for IS security research, and the theory could be fused with other theories to increase insight, in particular for studies that encompass socio-organizational and personal cognitive factors. This study offers initial evidence for the applicability of Bandura's triadic reciprocal determinism as a useful model to study IS security studies, and as data accumulates in the area, researchers may seek to examine full reciprocal determinism models. This study showed that self-efficacy commonly used for IS security studies using TPB, PMT, and others is pertinent to understanding behavioral outcomes in the area of IS security deviant behavior as well. This study's focus on NECISDB diversifies perspectives in the IS security literature. This study found the joint effect of self-regulation and self-efficacy to be an important factor that can influence employees' behavioral modification or change with regard to engagement in IS security malpractices. Attention is therefore drawn to the important role of the combined effect of self-efficacy and self-regulation in the management and control of NECISDB and related behaviors. Despite the flouring of work in the area of behavioral IS security research (e.g., Crossler et al., 2013; Sommestad et al., 2014), not many have recognized the relevance of self-regulation to the discourse. This study has practical implications as well. Given that observational learning/modeling can enhance self-efficacy, managers could task influential workers to act as champions of acceptable computing/IS with the belief that others will emulate their practices and actions. As the critical importance of the joint effect of self-regulation and self-efficacy on engagement in NECISDB is established, management could ensure that supportive resources, i.e., IS security awareness training and dedicated IT help desk are made readily available to employees who seek assistance in safe computing and information security practices. At the same time, measures to enhance individuals' self-regulation could be explored. For example, psychological counseling on how to improve IS security goal-setting standards could be instructive. Likewise, psychological evaluations could be conducted to assess workers' likelihood to engage in NECISDB. Such a test could provide initial information on how to manage workers likely to engage in NECISDB. Focused preventive strategies could then be developed, at an early stage, to deal with such.

Study's Limitations and Future Research Avenues

This study has its limitations. First, the data came from one region of the world; generalizing the study's findings to all parts of the world should be done with caution. Second, the data came from a cross-sectional field survey; longitudinal data may offer more insights. Third, items used to represent some of the study's constructs could be expanded. Fourth, the viewpoint of mid-level working professionals was used; generalizing the findings to all cohorts of workers may not be advisable. Future studies should overcome the noted shortcomings in this study. Future studies could include other SCT variables (e.g., outcome expectancy, social support) not considered here. As more data become available, future studies could explore Bandura's triadic reciprocal determinism in its full complement.

REFERENCES

Armerding, T. (2018). The 18 Biggest Data Breaches of The 21st Century. https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

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

Bandura, A. 1991. "Social Cognitive Theory of Self-Regulation," *Organizational Behavior and Human Decision Processes* (50:2), pp. 248-287.

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.

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

Chen, Y., Ramamurthy, K., and Wen, K.W. 2012. "Organizations' Information Security Policy Compliance: Stick Or Carrot Approach?," *Journal of Management Information Systems* (29:3), pp.157-188.

Corral-Verdugo, V. 1997. "Dual 'Realities' of Conservation Behavior: Self-Reports Vs Observations of Re-Use and Recycling Behavior," *Journal of Environmental Psychology* (17:2), pp. 135-145.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32:1), pp. 90-101.

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

Gist, M. 1987. "Self-efficacy: Implications for Organizational Behavior and Human Resource Management," *Academy of Management Review* (12:3) pp. 472-485.

Griffin, M. A. 1997. "Interaction Between Individuals and Situations: Using HLM Procedures to Estimate Reciprocal Relationships," *Journal of Management* 23(6), pp. 759-773.

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.

Guo, K.H., and Yuan, Y. 2012 "The Effect of Multilevel Sanctions on Information Security Violations: A Mediating Model," *Information & Management* (49:6), pp. 320-326.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2 Ed., Thousand Oaks, CA: Sage.

Ifinedo, P. 2014. "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. 2018. "Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions," *Information Resources Management Journal* (31:1), pp. 53-82

Ifinedo, P. 2019. "End User Nonmalicious, Counterproductive Computer Security Behaviors: Concept, Development, and Validation of an Instrument," *Security and Privacy*. https://onlinelibrary.wiley.com/doi/pdf/10.1002/spy2.66, pp. 1-13.

Hu, Q., Xu, Z., Dinev, T., and Ling, H. 2011. "Does Deterrence Work In Reducing Information Security Policy Abuse By Employees?," *Communications of the ACM* (54:6), pp. 54-60.

Jones, A. 2008. "Catching the Malicious Insider," *Information Security Technical Report* (13:4), pp. 220-224.

Kock, N. 2015. "Common Method Bias in PLS-SEM: A Full Collinearity Assessment Approach," *International Journal of e-Collaboration* (11:4), pp. 1-10.

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-Work-Related Personal Use of the Internet at Work," *Information & Management* (50:6), pp. 322-335.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior towards IS Security Policy Compliance," *in Proceedings of 40th Annual Hawaii International Conference*, Hawaii, USA.

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., 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.

Schunk, D. and Zimmerman, B. 2007. Influencing Children's Self-efficacy and Selfregulation of Reading and Writing through Modeling. *Reading & Writing Quarterly* (23:1), pp. 7-25.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J. 2014. "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies'," *Information & Management & Computer Security* (22:1), pp. 42–75.

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.

Tenenhaus, M., Vinzi V.E., Chatelin Y-M., and Lauro, C. 2005. PLS Path Modeling. *Computational Statistics and Data Analysis* (48:1), pp. 159–205.

Wetzels, M., Odekerken-Schröder, G., and Van Oppen, C. 2009. "Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration," *MIS Quarterly* (33:1), pp. 177-196.

van Vliet, J. (2018). Why Employees are the Biggest Threat to Company Data. https://www.information-age.com/employees-threat-123475710/.

Webb, T.L., and Sheeran, P. 2006. "Does Changing Behavioral Intentions Engender Bahaviour Change? A Metaanalysis of the Experimental Evidence," *Psychological Bulletin* (132:2), pp. 249–68.

Warkentin, M., and Willison, R. 2009. "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," *European Journal of Information Systems* (18:2), pp. 101–105.

Williams, G.C., Grow, V.M., Freedman, Z., Ryan, R.M., and Deci, E.L. 1996. "Motivational Predictors of Weight Loss and Weight-Loss Maintenance," *Journal of Personality and Social Psychology* (70:1), pp. 115-126.

Yi. M., 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.