Critical Times for Organizations: What Should Be Done to Curb Workers’ Noncompliance with Information Systems Security Policy Guidelines?

Princely Ifinedo

Department of Financial and Information Management, Shannon School of Business, Cape Breton University, P. O. Box 5300, Sydney, Nova Scotia B1P 6L2, Canada

DOI: 10.1080/10580530.2015.1117868

Abstract

This study was designed to examine the impacts of employees’ cost–benefit analysis, deterrence considerations, and top management support and beliefs on information systems security policy (ISSP) compliance. Surveys of Canadian professionals’ perceptions were carried out. A research model was proposed and tested. The results confirmed that top management support and beliefs, sanction severity, and cost–benefit analysis significantly influenced employees’ ISSP compliance. The implications of the study findings are discussed, and conclusions are drawn.

Keywords:
cost-benefit analysis, detection probability, information systems security policy (ISSP), sanction severity, structural equation modeling, top management beliefs and support

INTRODUCTION

Information systems (IS) and related technologies enable private and public organizations to store, process, and retrieve data and information assets in their daily operations (Laudon & Laudon, 2010). Organizations have since realized that competitive advantage can be built from such resources (Pearlson & Saunders, 2010). Despite the positive benefits accruing from IS resources, considerable risks are associated with their use in organizations (Keller, Powell, Horstmann, Predmore, & Crawford, 2005; Sumner, 2009; Westerman & Hunter, 2007). For example, security threats and breaches to an organization’s information assets can be a source of grave concern. In essence, the misuse or abuse of data and information held in an organization’s IS and related technologies can have dire consequences, such as financial loss, bad publicity, loss of credibility, as well as legal and regulatory problems (Bulgurcu, Cavusoglu, & Benbasat, 2010; Goel & Shawk, 2009; Guo, Yuan, Archer, & Connelly, 2011; Ifinedo, 2014; Siponen, Mahmood, & Pahnila, 2009). Recent IS security surveys and reports suggest that the
management and protection of information assets is fast becoming a critical concern for organizations as enormous costs are incurred in the attempt to safeguard such resources (Goel & Shawky, 2009; RichardSon, 2011; Hu, Dinev, Hart, & Cooke, 2012). Employees who fail to comply with their organizations’ information security guidelines and similar directives inadvertently facilitate the perpetration of computer crimes against their organizations. Computer crime encompasses a broad range of activities, including phishing scams. For example, an employee who does not heed his or her organization’s directives to shun scam emails or use strong passwords may endanger his or her organization’s data assets. Around the world, computer crimes and related activities cost organizations an average of over one trillion dollars annually (Hu, Xu, Dinev, & Ling, 2011).

In this critical time, what should organizations do to safeguard the information and other data assets held in their IS? Issues of this nature have emerged as a key concern of managers across the globe (Hu, Hart, & Cooke, 2007; Goel & Shawky, 2009; Siponen & Vance, 2010; RichardSon, 2011; Hu et al., 2012). Solutions that have been employed to address the problem often follow multi-perspective dimensions, i.e. technical and nontechnical approaches (Pahnila, Siponen, & Mahomood, 2007; Stanton, Stam, Mastrangelo, & Jolton, 2005; Vroom & von Solms, 2004). This is because focusing attention on one approach often does not yield the desired outcomes (Crossler et al., 2013; Ifinedo, 2014).

In this study, emphasis will be placed on the human aspects of organizational IS security issues as other researchers have sufficiently addressed relevant technical concerns (Crossler et al., 2013; Zafar & Clark, 2009). It is also worth pointing out that the IS security literature has consistently indicated that organizational employees (human agents) are, in fact, the weakest link with regard to ensuring IS security (Stanley et al., 2005; RichardSon, 2011; Hu et al., 2012; Harris, 2012; Harris & Furnell, 2012; Ifinedo, 2014). The human agent, either intentionally or unintentionally, engages in ill-prescribed behaviors that can endanger organizational IS resources (Harris & Furnell, 2012; Hu et al., 2011; Ifinedo, 2014; Pahnila et al., 2007; Siponen & Vance, 2010; Stanton et al., 2005).

Several organizations around the world have started developing organization-wide procedures, guidelines, or rules—sometimes commonly referred to as information systems security policy (ISSP) (Bulgurcu et al., 2010; Herath & Rao, 2009a; Siponen & Vance, 2010; Son, 2011)—or have implicitly defined such directives in other organizational documents (Ifinedo, 2012) to enable the control and management of such behaviors. Nevertheless, academic and industry reports have shown that even when ISSPs are in place, employees often do not readily comply with such documents (Harris & Furnell, 2012; Herath & Rao, 2009b; Pahnila et al., 2007; Siponen & Vance, 2010). For example, an employee may choose to not comply with his or her organization’s ISSP for reasons such as lack of top management support, inconvenience, ignorance, lack of appreciation for cost–benefit considerations, absence of organizational deterrence, and so forth (Bulgurcu et al., 2010; Cheng, Sims, & Teegen, 1997; D’Arcy & Herath, 2011; Herath & Rao, 2009b; Hu & Dinev, 2005; Hu et al., 2012; Son, 2011).

The following question then arises: What should organizations do to curb workers’ noncompliance with ISSPs and similar guidelines? This research is motivated by a desire to add to the debate with insights supported by an empirical study. Without a doubt, research is needed
to enhance our understanding of issues or factors that may inhibit or encourage employees’
compliance with their organizations’ ISSPs. Prior studies in the area have examined the
phenomenon from the perspective of a select few social psychology and criminology theories.
Research focusing on perceptions of top management support and beliefs and cost–benefit
analysis has not been widely represented in the literature. However, Bulgurcu et al. (2010) and
Li, Zhang, and Sarathy (2010) did examine the effect of cost–benefit analysis on ISSP
compliance behavior. Hu et al. (2012) studied top management support for promoting
employees’ ISSP compliance. Deterrence and sanctions have been widely discussed in previous
IS security research (see, e.g., D’Arcy et al., 2009; D’Arcy & Herath, 2011; Son, 2011; Straub,
1990).

In this study, it is argued that issues revolving around top management beliefs and support and
cost–benefit analysis, when duly considered alongside deterrence ones, could further engender
knowledge. Moreover, the literature indicates that no prior research has modeled all the
aforementioned constructs or factors in one study, hence their consideration in this research.
Given the suitability of the theory of planned behavior (Ajzen, 1991) in explicating all behaviors
and the fact that one of its tenets—that is, behavioral intention or intention to comply—has been
widely used in IS security literature (Bulgurcu et al., 2010; Chan, Woon, & Kankanhalli, 2005;
Herath & Rao, 2009b; Ifinedo, 2012; 2014; Pahnila et al., 2007), it was decided to accordingly
utilize behavioral intention as the dependent variable of this research.

The remainder of the paper is organized as follows. First, background information on IS security
compliance and relevant theoretical underpinnings are succinctly presented. Next, the research
model and hypotheses are formulated. Discussions on research methodology follow. Thereafter,
the data analysis section is presented. Finally, the study findings and results are discussed and
relevant concluding remarks made.

BACKGROUND LITERATURE

The phenomenon of ISSP compliance or noncompliance in the workplace is emerging as an
integral part of the burgeoning behavioral IS security management literature (Crossler et al.,
information security behaviour refers to the set of core information security activities that have to
be adhered to by end-users to maintain information security as defined by information security
policies.” Given the critical value of information and data assets to organizations, it is crucial to
pay attention to workers’ behavior with respect to IS security issues. Kolkowska & Dhillon,
2013, p. 374) commented that “the security behavior of users is integrated in, and enacted
through, the daily activities of their practice” in the workplace. As such, ISSP security
compliance research aims at increasing understanding of the issues or factors influencing
employees’ compliance/noncompliance with their organizations’ ISSPs.

Useful insights are beginning to emerge. For example, Hone and Eloff (2002) suggested that
employees’ behavior and attitudes toward information security issues benefit from top
management beliefs. Herath and Rao (2009a) showed that organizational commitment
significantly impacted IS security policy compliance. Li et al. (2010) provided information as to
the relevance of cost–benefit analysis to compliant IS behavior. Bulgurcu et al. (2010) reported
that the costs and benefits of compliance and the costs of noncompliance have positive influences on end-user attitudes toward compliance and intention to comply with ISSPs. While some researchers (e.g., D’Arcy et al., 2009; Hovav & D’Arcy, 2012; Straub & Welke, 1998) indicated that deterrence factors (sanctions and detection probability) mattered for ISSP compliance and related behavior, others (e.g., Hu et al., 2011; Son, 2011) failed to find support for the same view. Further still, other researchers that used deterrence factors to study ISSP compliance behavior reported mixed and confusing results (e.g., 2009b; Herath & Rao, 2009a; Li et al., 2010). Specifically, this study aims at contributing to the growing body of work in the area by using empirical data sourced from working professionals. In addition, this study augments prior studies that used scenario-based approaches to investigate comparable phenomena (e.g., Guo et al., 2011).

**Theoretical Underpinnings**

**General Deterrence Theory**

General deterrence theory (GDT) was originally developed to dissuade people from committing antisocial acts or engaging in undesirable activities through the use of countermeasures, such as strong disincentives and sanctions (Chiricos & Waldo, 1970). Straub and Welke (1998) introduced the theory to the IS domain. The two pillars of GDT are sanction severity and detection probability. Sanction severity refers to the harshness of penalties for engaging in deviant behavior—that is, noncompliance with an organization’s ISSP (Herath & Rao, 2009a). Detection probability refers to the likelihood of being caught violating IS policies or rules (Son, 2011). Empirical findings regarding the relationship between GDT’s sub-constructs and ISSP compliance have been mixed (D’Arcy & Herath, 2011; Hovav & D’Arcy, 2012). For example, while some researchers (e.g., Herath & Rao, 2009a, 2009b; Li et al., 2010) found aspects of GDT—i.e. deterrence—to be linked to employees’ ISSP compliance, others failed to confirm such relationships (e.g., Hu et al., 2011; Son, 2011).

**Rational Choice Theory**

The concept of cost–benefit analysis, which is anchored in rational choice theory (RCT), has been extended to a wide range of areas, including organizational crime (Becker, 1968; Paternoster & Simpson, 1968). Cost–benefit analysis refers to the technique that is used to determine the best approaches from a set of alternatives (Boardman, 2006). Essentially, RCT offers explanations as to how humans make decisions in a rational manner when faced with choices. The theory posits that people will seek the most cost-effective means to achieve a specific goal. Citing Paternoster and Simpson (1996), Li et al. (2010) noted that the decision by an offender to engage in an antisocial or deviant act may be hinged upon some subjective expectations of benefits and costs as well as the perceived balance between both indicators.

**Organizational Climate Perspective**

Organizational climate (OC) refers to a set of properties in the work environment that directly or indirectly affects employees’ behavior (Schneider, Brief, & Guzzo, 1996). Drawing upon the OC literature, Chang and Lin (2007) showed that a strong perception of environmental factors helps
to curb employees’ noncompliant IS behaviors. It is worth noting that OC may include a variety of issues, such as top management beliefs and support, facilitating conditions, and employees’ beliefs and attitudes. For the purposes of this study, focus will be on top management beliefs and support. Past research has examined the effects of facilitating conditions and employees’ attitudes on ISSP compliance (e.g., Guo et al., 2011; Pahnila et al., 2007); however, focus on top management beliefs and support has been rare (Hu et al., 2012).

In this study, top management support and beliefs regarding IS security issues refers to the extent to which top managers in the organization provide direction, authority, and resources related to IS security concerns. Schneider et al. (1996) suggested that the beliefs and practices of management often make a significant difference in shaping the opinions of workers. In climates or contexts in which the management publicly supports an IS-based initiative, organizational members usually interpret such moves positively and act accordingly. Young and Windsor (2010) noted the importance of top management support for information security planning, and Hu et al. (2012) found that workers’ compliance with organizations’ information security is positively influenced by top management support.

THE RESEARCH MODEL AND HYPOTHESES

The proposed research model is shown in Figure 1. It includes the aforementioned factors discussed in the foregoing section. The control variables, such as age, gender, education, occupation (IS and non-IS), organizational size (workforce and revenue), and the availability of formal/informal ISSPs, were included to enhance insight. Prior research conducted by Herath and Rao (2009a) and Hovav and D’Arcy (2012) found that age and gender differences mattered when it came to employees’ ISSP compliance and IS misuse intention. Lee and Larsen (2009) found that the adoption intention of IS experts and non-IS professionals differed significantly with respect to accepting protective security tools. Employees’ positions (rank) were found to have a positive impact on ISSP compliance (Guo & Yuan, 2012). Discussions on the research hypotheses are presented next.
Figure 1. The research model.

Top management support and beliefs are important ingredients in enforcing governance and responsibility vis-à-vis information security issues in organizations (Herath, Herath, & Bremser, 2010; Von Solms & Von Solms, 2004). Employees’ beliefs tend to be influenced by the conduct, views, and perceptions of top management (Chang & Lin, 2007; Philip, 2007). Likewise, employees’ views on IS security issues in organizations are influenced by top management support and concerns (Hu et al., 2012; Puhakainen & Siponen, 2010). It has been established that when top management support for IS security issues is high, compliance with ISSPs is correspondingly high (Chang & Lin, 2007; Hu et al., 2012). Thus, it is hypothesized that:

**H1:** Top management support and beliefs related to IS security issues will positively influence employees’ compliance with ISSPs.

In general, individuals become reticent to comply with recommendations if they believe that a considerable amount of resources—that is, time, effort, and money—will be expended on such an effort (Lee & Larsen, 2009; Milne et al., 2000). Contrastingly, if small amounts of resources are required to implement a measure, compliance tends to be warmly received (Pechmann, Zhao, Goldberg, & Reibling, 2003; Workman, Bommer, & Straub, 2008). In other words, a balance between cost and benefit considerations for a particular effort tends to bode well for accepting individuals (Ifinedo, 2012; Li et al., 2010). Past studies found that cost–benefit assessment is negatively related to intention to use IS security measures and policies (Lee & Larsen, 2009; Li et al., 2010; Workman et al., 2008). Hu and Dinev (2005) noted that if individuals are aware of the potential damage that malware could cause, they tend to be proactive in taking protective actions. Thus, it is hypothesized that:

**H2:** Cost–benefit analysis of IS security issues will negatively influence employees’ compliance with ISSPs.
Straub (1990) showed that stating the penalties and sanctions for ISSP noncompliance increased individuals’ acceptable security behaviors. Penalties for noncompliance, such as job loss, demotion, fines, and other severe disciplinary actions, may enhance desired IS security behaviors (Herath & Rao, 2009b). Past research has suggested that shaming offenders may serve to encourage security compliance (Harris & Furnell, 2012). While some researchers (Hu et al., 2011; Pahnila et al., 2007; Son, 2011) have not confirmed the existence of a positive relationship between sanctions and ISSP compliance, several others have done so (please see, e.g., D’Arcy & Herath, 2011). We accept that where appropriate sanctions are in place and enforced, the urge to comply with ISSPs will be high. Thus, it is hypothesized that:

**H3**: Sanction severity will positively influence employees’ compliance with ISSPs.

The antisocial behavior of illegally copying software was reported to be high when the probability of being caught was perceived to be low by perpetrators (Cheng et al., 1997). Likewise, high perceived detection probability decreased noncompliance with Internet use policy (Li et al., 2010). Noncompliance with the ISSP is high when such rules are not enforced or when an individual worker knows that he or she cannot be detected (Herath & Rao, 2009b). The study by Herath and Rao (2009a) showed that when employees knew they were being monitored and their chances of getting away with noncompliance with their organizations’ ISSPs were low, they tended to be more willing to comply with such policies. Ceteris paribus, if the probability of detection increases, employees’ noncompliance with ISSPs will decrease. Thus, it is hypothesized that:

**H4**: Detection probability will negatively influence employees’ noncompliance with ISSPs.

**THE RESEARCH METHODOLOGY**

**Study Design and Data Collection**

As was done in the majority of the prior research in this area, a field survey was used to collect the data. Whenever possible, the measurement items of the constructs were taken from validated scales in the extant literature. The developed questionnaire was pretested by 10 individuals, including college professors and working professionals familiar with ISSPs in their organizations. Two approaches were used to collect the data for the research; both paper and online questionnaires were used to administer the final questionnaire.

First, a directory containing the names and addresses of 1,000 non-IS managers in Canadian organizations was purchased from the marketing and data research firm, InfoCanada. A cover letter, questionnaire, and self-addressed stamped envelope were mailed to each contact on the list. Of the 1,000 questionnaires mailed, 131 were undelivered. The 94 responses that were received reflect an effective response rate of 10.8% from this particular source. The response rate from this source is relatively high given the problems that are typically encountered when collecting security-related data from organizations (Kotulic & Clark, 2004). Eleven responses were excluded from the 94 received responses for various reasons, including monotone or
patterned responses and many missing answers on the questionnaire; thus, 83 responses was retained from this source.

Second, to increase knowledge of ISSP compliance in organizations, the views of IS professionals were also sampled as was done by previous researchers (e.g., Herath & Rao, 2009a; Lee & Larsen, 2009). Past studies have suggested that IS professionals and business managers assess IS-related issues differently (e.g., Ifinedo & Nahar, 2007; Lee & Larsen, 2009). By including the viewpoints of both cohorts, the generalizability of the study findings and conclusions is accordingly enhanced. That said, it is impossible to procure a list of IS professionals in Canada; therefore, the decision was made to use judgmental and convenience sampling (Iacobucci & Churchill, 2009) to collect data from such professionals. Contact was made with the relevant managers of the Canadian Association of Information Technology Professionals (CIPS), who agreed to direct their members to an online version of the same questionnaire previously mailed to non-IS managers. The managers of CIPS noted that, due to administrative directives, the association cannot provide details of its membership. Nonetheless, members of the CIPS received communication from their managers that included a web link to our online-based survey (hosted by QuestionPro.com). Fifty-five CIPS members completed the online survey; four responses were excluded for reasons already noted, which left 51 acceptable responses from this source.

Additionally, 60 Canadian (non-IS and IS) professionals from locations across the country who are connected with the researchers on the social network site LinkedIn were asked to complete the survey online. Forty-four contacts from this source completed the survey online for an effective response rate of 73%; however, two responses were not used due to their many missing answers. Thus, 42 responses were obtained from this particular source.

All the participants were motivated by four $100 gift certificates and a promise to share the summary of the results with them. Participation in the study was voluntary, and respondents were assured that individual responses would be anonymous and confidential. Thus, a total of 176 (i.e., 83 + 51 + 42) usable responses from the varied sources were used to validate the constructs and test the hypotheses. It is worth noting that the data sample size is comparable to those used in similar studies in the literature (e.g., Chan et al., 2005; Ng, Kankanhalli, & Xu, 2009). As the unit of analysis was the individual employee, the concern of respondent error—that is, common method bias (CMB)—cannot be ruled out. CMB refers to a bias in the dataset due to factors external to the measures used for the study. This study contained such biases by soliciting participation from employees with diverse backgrounds—that is, occupation, firm size, and industry. With such heterogeneity in our data sample, the potential for biases arising from concerns diminishes. Regardless, the procedural remedies for controlling CMB, as recommended by Podsakoff, MacKenzie, Lee, and Podsakoff (2003), were followed; namely, clear and concise questions were used in the questionnaire to reduce participants’ apprehension, and, as noted above, their anonymity was assured. In addition, a statistical procedure—that is, the Harman’s single factor test—was used to assess whether CMB was problematic for the data sample (Podsakoff et al., 2003). The test results showed that five factors with eigenvalues greater than one are present in the data. The first factor accounted for 31.7% of the total variance to indicate a lack of evidence of a substantial CMB in the study data.
In testing for nonresponse bias in the research sample, the procedure recommended by Armstrong and Overton (1977) was used. Namely, early and late respondents from both the mail and online surveys were compared on several individual and organizational demographic measures, including gender, age, occupation, job tenure, and organization size. The analysis of variance (ANOVA) tests that were conducted did not find statistical differences between the survey’s nonparticipants (late respondents) and participants (early respondents) on the measures used. Additionally, the respondents were classified by the sampling techniques used—that is, random and otherwise. The independent t-tests used to compare early and late responses from the sampling techniques for various individual and organizational demographic measures did not indicate statistical differences between both groupings. Together, these tests strengthen the claim for a lack of nonresponse bias in the data sample.

Table 1 presents information about the respondents’ demographic; it includes a balanced mixture of 81 males (46%) and 95 females (54%) with many of them having a university education. There were 110 (62.5%) non-IS managers and 66 (37.5%) IS professionals in the sample. On average, the respondents had 7.7 years (S.D. = 7.5) of tenure at their current organizations. Some of the job titles of the IS professionals included IS directors, chief information officers, and IS project managers. Of the non-IS managers, there were chief human resources officers, vice presidents of marketing, and key account managers. Diverse industries were also included in the sample; their annual revenue ranged from $500,000 to over $100 million.

Table 1. Demographic characteristics of the sample (N = 176) (Contd.)

<table>
<thead>
<tr>
<th>Demographic variable</th>
<th>Category</th>
<th>Frequency</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Less than 20 years</td>
<td>2</td>
<td>1.1</td>
</tr>
<tr>
<td></td>
<td>21- 30 years</td>
<td>28</td>
<td>15.9</td>
</tr>
<tr>
<td></td>
<td>31- 40 years</td>
<td>40</td>
<td>22.7</td>
</tr>
<tr>
<td></td>
<td>41-50 years</td>
<td>50</td>
<td>28.4</td>
</tr>
<tr>
<td></td>
<td>50 - 60 years</td>
<td>44</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>61 years and above</td>
<td>8</td>
<td>4.5</td>
</tr>
<tr>
<td></td>
<td>Missing</td>
<td>4</td>
<td>2.3</td>
</tr>
<tr>
<td>Education</td>
<td>Secondary education</td>
<td>4</td>
<td>2.3</td>
</tr>
<tr>
<td></td>
<td>Vocational/technical</td>
<td>29</td>
<td>16.5</td>
</tr>
<tr>
<td></td>
<td>University education</td>
<td>103</td>
<td>58.5</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>34</td>
<td>19.3</td>
</tr>
<tr>
<td></td>
<td>Missing</td>
<td>6</td>
<td>3.4</td>
</tr>
<tr>
<td>Rank (Position)</td>
<td>Top management personnel</td>
<td>41</td>
<td>23.3</td>
</tr>
<tr>
<td></td>
<td>Mid-level personnel</td>
<td>111</td>
<td>63.1</td>
</tr>
<tr>
<td></td>
<td>Junior staff</td>
<td>18</td>
<td>10.2</td>
</tr>
<tr>
<td></td>
<td>Missing</td>
<td>6</td>
<td>3.4</td>
</tr>
<tr>
<td>Availability of ISSPs: (Explicit/Implicit)</td>
<td>Yes</td>
<td>103</td>
<td>58.5</td>
</tr>
<tr>
<td></td>
<td>Expressed in other organizational documents</td>
<td>61</td>
<td>34.7</td>
</tr>
<tr>
<td></td>
<td>Don’t know</td>
<td>12</td>
<td>6.8</td>
</tr>
<tr>
<td>Industry</td>
<td>Manufacturing</td>
<td>20</td>
<td>11.4</td>
</tr>
<tr>
<td></td>
<td>Retail/Wholesale</td>
<td>28</td>
<td>15.9</td>
</tr>
<tr>
<td></td>
<td>Education</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Telecoms/High Tech/IT</td>
<td>23</td>
<td>13.1</td>
</tr>
</tbody>
</table>
Operationalization of the Research Constructs

The items used to operationalize detection probability and sanction severity were taken from Li et al. (2010). The behavioral intentions (BEHI) scale had measures modified from Herath and Rao (2009a, 2009b) and Ifinedo (2012). The items used to operationalize top management support and beliefs benefited from discussions in Schneider et al. (1996). The cost–benefit analysis was adapted from Workman et al. (2008) and Ifinedo (2012). The majority of the measurement items were anchored on a 7-point Likert scale ranging from “strongly disagree” (1) to “strongly agree” (7), in which participants were asked to indicate an appropriate response. The constructs and their descriptive statistics are provided in Table 2.

Table 2. The questionnaire’s items, their descriptive statistics, and item loadings (Contd.)

<table>
<thead>
<tr>
<th>Construct</th>
<th>Item</th>
<th>M</th>
<th>Sd</th>
<th>Loading (t value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOPM</td>
<td>Management is concerned about employee involvement in IS security issues.</td>
<td>5.32</td>
<td>1.39</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Top management thinks everyone should adhere to the organization’s IS security policy.</td>
<td>5.99</td>
<td>1.11</td>
<td>0.8615 (10.086)</td>
</tr>
<tr>
<td></td>
<td>Top management believes that the organization’s IS security policy provides significant business benefits to the firm.</td>
<td>5.82</td>
<td>1.25</td>
<td>0.8703 (7.824)</td>
</tr>
<tr>
<td></td>
<td>My organization’s administration efficiently deals with information security issues.</td>
<td>5.64</td>
<td>1.28</td>
<td>NA</td>
</tr>
<tr>
<td>DETC</td>
<td>The probability that I would be caught if I failed to comply with my organization’s IS security</td>
<td>4.05</td>
<td>1.98</td>
<td>1.00000 (0.000)</td>
</tr>
<tr>
<td>M</td>
<td>Sd</td>
<td><strong>I can easily bypass my organization’s IS security policy guidelines without being caught</strong></td>
<td>3.03</td>
<td>1.92</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td><strong>SANC</strong></td>
<td><strong>M =</strong></td>
<td>If I were caught not adhering to my organization’s IS security policy directives, I think the punishment would be:</td>
<td>4.66</td>
<td>2.14</td>
</tr>
<tr>
<td><strong>Sd =</strong></td>
<td></td>
<td>If I were caught not adhering to my organization’s IS security policy directives, I would be severely punished by my organization</td>
<td>5.01</td>
<td>1.93</td>
</tr>
<tr>
<td><strong>COSB</strong></td>
<td><strong>M = 3.75</strong></td>
<td>There are too many overhead costs associated with implementing IS security measures in my organization:</td>
<td>3.67</td>
<td>1.75</td>
</tr>
<tr>
<td><strong>Sd = 1.74</strong></td>
<td></td>
<td>Enabling IS security measures in my organization is/would be time consuming:</td>
<td>3.84</td>
<td>1.68</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The inconvenience of implementing recommended IS security policy measures is:</td>
<td>3.73</td>
<td>1.78</td>
</tr>
<tr>
<td><strong>BEHI</strong></td>
<td><strong>M =</strong></td>
<td>I would follow the organization’s IS security policy whenever possible</td>
<td>6.19</td>
<td>1.03</td>
</tr>
<tr>
<td><strong>Sd =</strong></td>
<td></td>
<td>I am certain I will adhere to my organization’s IS security policy</td>
<td>6.06</td>
<td>1.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It is possible that I will comply with the organization’s IS security policy to protect the organization’s information systems</td>
<td>6.12</td>
<td>1.19</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It is my intention to continue to comply with the organization’s IS security policy</td>
<td>6.25</td>
<td>1.11</td>
</tr>
</tbody>
</table>

**Notes:**

a) M = mean; Sd = standard deviation; NA = not applicable
b) The measuring variables indicated with italicized texts was deleted from further data analysis due to their low item loadings.
c) This items was assessed with the following scale: Very low = 1 … Neutral = 4 … Very high = 7.
d) This item was assessed with the following scale: Not very serious = 1 … Neutral = 4… Very serious = 7.
e) This item was assessed with the following scale: Lower than the benefits = 1 … Neutral = 4… Exceeds the benefits = 7.

**DATA ANALYSIS**

The partial least squares (PLS) technique of structural equation modeling (SEM), which utilizes a principle component-based for estimation, was used for analysis (Chin, 1998; Tenenhaus, Esposito Vinzi, Chatelinc, & Lauro, 2005). The PLS technique places minimal demands on sample size and residual distributions. The ad hoc rule of thumb for using PLS is that the sample size should be at least 10 times the largest number of structural paths directed at a particular latent construct in the structural model (Chin, 1998). In this regard, a sample size of 40 would be considered adequate for this study; however, the study sample is 176. The PLS software used in this study was SmartPLS 2.0 (Ringle, Wende, & Will, 2005). PLS offers information regarding the assessment of the measurement and structural models.
Measurement Model

In assessing the psychometric properties of a model, the following indicators are used: internal consistency as well as convergent and discriminant validities. To assess internal consistency reliability, the Cronbach alpha coefficients and composite reliability indicators provided by SmartPLS 2.0 are used. A Cronbach alpha value of 0.5 or more is usually considered acceptable (Hair, Anderson, & Thatham et al., 1998). The results in Table 3 show reasonably high values on all the constructs. Convergent validity captures the extent to which a measure correlates with the other measures with which it is theoretically predicted to correlate. It is assessed by two criteria. First, item loadings greater than 0.7 indicate strong convergent validity results (Fornell & Larcker, 1981); however, values greater than 0.5 are also acceptable for exploratory studies (Hair et al., 1998). Second, the square root of the average variance extracted (AVE) for a construct is observed to determine whether it is able to explain at least half (50%) of the measures’ variance (Fornell & Larcker, 1981). The results in Table 3 meet these criteria as well.

Table 3. Composite reliability, Cronbach alpha, AVE, and inter-construct correlations

Table 3: Composite reliability, Cronbach alpha, AVE, and Inter-construct Correlations

<table>
<thead>
<tr>
<th>Construct</th>
<th>CR</th>
<th>AVE</th>
<th>DETC</th>
<th>BEHI</th>
<th>TOPM</th>
<th>COSB</th>
<th>SANC</th>
</tr>
</thead>
<tbody>
<tr>
<td>DETC</td>
<td>NA</td>
<td>NA</td>
<td>1.00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BEHI</td>
<td>0.96</td>
<td>0.86</td>
<td>0.28</td>
<td>0.93</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOPM</td>
<td>0.86</td>
<td>0.75</td>
<td>0.29</td>
<td>0.31</td>
<td>0.87</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COSB</td>
<td>0.74</td>
<td>0.51</td>
<td>-0.16</td>
<td>-0.25</td>
<td>-0.14</td>
<td>0.71</td>
<td></td>
</tr>
<tr>
<td>SANC</td>
<td>0.82</td>
<td>0.69</td>
<td>0.53</td>
<td>0.45</td>
<td>0.38</td>
<td>-0.06</td>
<td>0.83</td>
</tr>
</tbody>
</table>

Notes:
a) Composite reliability (CR), Average variance extracted (AVE); Not applicable (NA)
b) The bold fonts in the leading diagonals are the square root of AVEs;
c) Off-diagonal elements are correlations among latent constructs; the acronyms are defined in the text.

Table 4. Summary of the results

<table>
<thead>
<tr>
<th>Hypothesized path</th>
<th>β</th>
<th>t-value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top management support/beliefs → ISSP behavioral intention</td>
<td>0.07</td>
<td>0.575</td>
<td>H1: Supported</td>
</tr>
<tr>
<td>Costs/benefits analysis (-) → (ISSP behavioral intention</td>
<td>0.04</td>
<td>0.395</td>
<td>H2: Supported</td>
</tr>
<tr>
<td>Sanctions → ISSP behavioral intention</td>
<td>0.41</td>
<td>2.571</td>
<td>H3: Supported</td>
</tr>
<tr>
<td>Detection probability (-)→ ISSP behavioral intention</td>
<td>-0.17</td>
<td>2.029</td>
<td>H4: Not supported</td>
</tr>
</tbody>
</table>

Notes: ➔ = positive relationship; (-) ➔ = negative relationship

Discriminant validity measures the degree to which constructs are distinct or diverge from one another. The discriminant validity of the constructs used in this study is gauged in three ways. First, a minimum value of 0.5 for a construct’s AVE is recommended by Fornell and Larcker (1981). All the AVE values in Table 3 were above 0.50, which suggests that the principal constructs capture a much higher construct-related variance than error variance. Second, it is also
recommended that the square root of the AVE of the multi-item reflective constructs be greater than the absolute value of the inter-construct correlations in the model (Fornell & Larcker, 1981). Table 3 shows that the square roots of the AVEs (in the diagonal element) were larger than all other cross-correlations. Third, the cross-loadings of the constructs were checked (Chin, 1998; Hair et al., 1998). The results in this regard indicated that all measuring items exhibited high loadings on their own respective constructs, and no indicators loaded higher on other constructs that were not theoretically designed to represent them (see the appendix). Thus, the results indicated that the study measures were psychometrically adequate.

**Structural Model**

After establishing reliability, validity, and the absence of common method variance, the structural model was assessed. The structural model presents information about the path significance of hypothesized relationships using the path coefficients (β) and squared R (R²). The SmartPLS 2.0 results for the βs and the R² are shown in Figure 2. A bootstrapping procedure with 1,000 samples was used to assess the path significance levels (t-values).

Figure 2. The PLS results.

Hypothesis H1, which suggested that top management support and beliefs would positively influence employees’ behavioral intention to comply with ISSP guidelines, was supported (β = 0.16). The data confirmed hypothesis H2, which predicted that cost–benefit analysis would negatively influence employees’ ISSP behavioral intention (β = −0.21). Hypothesis H3, which
predicted that sanction severity would positively influence employees’ behavioral intention to comply with ISSP guidelines, was strongly supported by the data ($\beta = 0.37$). Hypothesis H4, which predicted that detection probability would negatively impact employees’ behavioral intention to comply with ISSP guidelines, was unconfirmed ($\beta = 0.02$). All the constructs explained 30% of the variance in ISSP behavioral intention, which is acceptable for an exploratory study such as this one. It is worth mentioning that none of the control variables—age, education, occupation (IS and non-IS professionals), job rank, survey method, and so forth—had statistical significance in the research model.

A plausible explanation for the unsupported hypothesis might be due to the research design and possibly other contextual or extraneous influences. For instance, D’Arcy and Herath (2011) indicated that more needs to be done with regard to the measures usually used to operationalize deterrence constructs—that is, detection probability in IS security research. Further to this, recent studies (e.g., Siponen & Vance, 2010) have suggested that employees use a variety of means, including neutralization techniques to circumvent compliance with organizations’ IS rules. As a consequence, the likelihood of being caught not adhering to organizations’ ISSP rules did not serve to deter employees’ noncompliance (Hu et al., 2011; Son, 2011). The result obtained herein seems, to some extent, to reflect similar observations reported in prior research.

**DISCUSSIONS AND CONCLUSION**

This study was designed to enlighten understanding of what needs to be done to curb workers’ noncompliance with ISSP guidelines in the present era in which the misuse or abuse of IS assets can be disastrous for organizations. While it is not claimed that the findings of this research are the final word on the topic, it is hoped that the suggestions offered herein will add to the growing body of knowledge in the area. The theoretical contributions and practical implications of this research effort are presented as follows.

**Theoretical Contributions of the Study**

First, this study’s proposed research conceptualization, which considered the effects of top management support and beliefs, cost–benefit analysis, and GDT, diversifies insights and complements prior understanding in the area. Second, it offers an alternative perspective to understanding employees’ ISSP behavioral intentions in the sense that the impacts of more than one factor or influence are examined. The attention of researchers is accordingly kindled. For example, other relevant factors (e.g., reward, shame, and employees’ security beliefs) could be incorporated into the research model to further engender understanding of what might help curtail employees’ ISSP noncompliance in the workplace. Third, this study provides further empirical evidence for the pertinence of top management support and beliefs, sanctions, and cost–benefit analysis to compliance with information security rules in work settings (e.g., Hu et al., 2012; Lee & Larsen, 2009; Li et al., 2010; Straub, 1990; Workman et al., 2008). It emphasizes the fact that acceptable security compliance behaviors can be positively impacted by a rational assessment of cost–benefit imperatives, deterrence mechanisms in the form of sanctions, and support from top management. These findings lend credence to the views of others discussing similar themes in the literature. Fourth, this study provides further proof of the applicability and suitability of OC perspectives, RCT, and, to some extent, GDT to the study of
employees’ compliance behavior. Fifth, this study supports the view espoused by others suggesting that deterrence—that is, detection probability—may not be useful for discouraging employees’ noncompliance with organizations’ ISSPs and related rules.

**Practical Implications of the Study**

This research has several important implications for practitioners. The study results showed that an employee’s noncompliance or compliance with ISSP guidelines may be circumscribed by the individual’s rational choice. To encourage compliance with such rules, it may be advisable for management to find ways of proactively communicating to their workers the importance of adhering to acceptable IS security. Namely, information about the benefits and advantages that workers stand to gain from compliance should be made clear. For instance, hefty liabilities incurred by the organization through the activities of sloppy or careless workers who fail to follow IS security rules could result in firm closure and demise. Likewise, employees should be shown that while complying with proper IS behaviors could appear time-consuming in the short term, both the organization and the workers stand to reap positive benefits in the long term. Given the importance of top management support and beliefs in shaping opinions and attitudes toward organizational issues, it may be advisable for top managers to develop a hands-on approach to implementing, promoting, and enforcing rules supported in their ISSPs. Rather than delegate the implementation and enforcement of information security rules to the IS department and others (US GAO, 1998), as management would prefer, they should be visibly active in all the processes associated with developing and enforcing security procedures in their organizations.

Practitioners can engender employees’ ISSP behavioral intentions by fostering a climate in which appropriate sanctions and penalties are instituted. It is important to temper the foregoing statement by noting that any penalty meted out to deviant employees has to be measured; recent research has shown that applying sanctions without such considerations may lead to counterproductive outcomes (e.g., Geddes & Stickney, 2010). That said, it is maintained that sanctions can discourage an employee’s noncompliance with ISSP guidelines insofar as the individual’s concerns and the organization’s concerns and liabilities are adequately understood. It is suggested that employees would not comply with their organizations’ ISSPs merely by being deterred by detection mechanisms. Rather, the incorporation of such effort with other procedures may be required to achieve the necessary outcomes. Put differently, practitioners may not elicit acceptable employees’ IS security compliance behavior by focusing on detection tools alone. In particular, enterprise-wide education on IS security issues can be put in place to help achieve such favorable outcomes. Top managers’ lead may be a sine qua non in such matters.

**Limitations of the Study and Avenues for Future Research**

First, the research included the views of respondents who have formal ISSPs in their organizations as well as those without such guidelines. The inclusion of both might have negatively impacted the results; however, it was ensured that participants from organizations with no formal ISSPs understood the meaning of ISSPs and/or organizations’ IS rules regarding acceptable IS security behaviors. Importantly, the comparisons of both groupings’ responses did not indicate significant statistical differences between the two. Second, the sample was not
completely random; this might have negatively impacted the generalizability of the study findings. Nonetheless, comparisons of data obtained from the various sources used in the study did not indicate differences of opinion among the participants. Third, although common method bias was not a problem in this study, it is still possible that participants might have provided “socially desirable responses” to some of the issues being investigated. Fourth, the research data came from a cross-sectional field survey; longitudinal data may facilitate more insight. Fifth, items used to operationalize some of the study constructs could be expanded.

Future studies in the area could overcome some of the limitations of our research. For example, the construct of detection probability could be upgraded with the addition of more measuring items. Future research could consider investigating ISSP behavioral compliance using qualitative approaches such as in-depth interviews and focus groups to enrich insight. In the future, other variables, such as personality types and characteristics, subjective norms, shame, rewards, and so forth, could be considered. Lastly, other relevant theories, such as organization citizenship behavior and organizational learning, could be incorporated into the research model to enhance knowledge.

Acknowledgments

Funding for this study was obtained from the research policy (RP) grants of Cape Breton University, Canada. Special thanks go to Messrs. Ringle, C.M., Wende, S. and Will, A. for the use of their software, SmartPLS 2.0. The author appreciates the comments and suggestions provided by anonymous reviewers of an earlier draft of this paper.

Author biographies

Princely Ifinedo is an Associate Professor at Cape Breton University, Canada. He holds a PhD in Information Systems (IS) from University of Jyväskylä, Finland, an MBA from the Royal Holloway, University of London, UK, and a M.Sc. from Tallinn University of Technology, Estonia. His research includes ERP success and IS security management. He has presented at various IS conferences, contributed chapters to several books/encyclopedias, and published in journals such as I&M, JCIS, C&S, JSS, DATA BASE, CHB, JITM, IMDS, EIS, JGTIM, JISP, and Internet Research. He has authored over 100 peer-reviewed publications and he is affiliated with AIS and CIPS.
Appendix. Cross Loadings of the Constructs

<table>
<thead>
<tr>
<th></th>
<th>DETC</th>
<th>BEHI</th>
<th>TOPM</th>
<th>COSB</th>
<th>SANC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behi1</td>
<td>0.281005</td>
<td><strong>0.93473</strong></td>
<td>0.308568</td>
<td>-0.26709</td>
<td>0.377919</td>
</tr>
<tr>
<td>Behi2</td>
<td>0.299667</td>
<td><strong>0.952394</strong></td>
<td>0.337873</td>
<td>-0.23865</td>
<td>0.447</td>
</tr>
<tr>
<td>Behi3</td>
<td>0.242025</td>
<td><strong>0.918198</strong></td>
<td>0.258009</td>
<td>-0.26298</td>
<td>0.398787</td>
</tr>
<tr>
<td>Behi4</td>
<td>0.226267</td>
<td><strong>0.904956</strong></td>
<td>0.243569</td>
<td>-0.15042</td>
<td>0.429726</td>
</tr>
<tr>
<td>Detc1</td>
<td>1</td>
<td>0.284</td>
<td>0.287055</td>
<td>-0.15743</td>
<td>0.525376</td>
</tr>
<tr>
<td>Topm2</td>
<td>0.200974</td>
<td>0.268805</td>
<td><strong>0.867052</strong></td>
<td>-0.20127</td>
<td>0.289283</td>
</tr>
<tr>
<td>Topm3</td>
<td>0.297166</td>
<td>0.271691</td>
<td><strong>0.870072</strong></td>
<td>-0.04742</td>
<td>0.37783</td>
</tr>
<tr>
<td>Cosb1</td>
<td>0.042193</td>
<td>-0.14247</td>
<td>-0.02181</td>
<td><strong>0.720933</strong></td>
<td>0.096935</td>
</tr>
<tr>
<td>Cosb2</td>
<td>-0.14497</td>
<td>-0.17018</td>
<td>-0.04423</td>
<td><strong>0.761061</strong></td>
<td>-0.10684</td>
</tr>
<tr>
<td>Cosb3</td>
<td>-0.18767</td>
<td>-0.19595</td>
<td>-0.20214</td>
<td><strong>0.611826</strong></td>
<td>-0.08062</td>
</tr>
<tr>
<td>Sanc1</td>
<td>0.599841</td>
<td>0.32576</td>
<td>0.321294</td>
<td>-0.07575</td>
<td><strong>0.788219</strong></td>
</tr>
<tr>
<td>Sanc2</td>
<td>0.310036</td>
<td>0.40904</td>
<td>0.320345</td>
<td>-0.02556</td>
<td><strong>0.871665</strong></td>
</tr>
</tbody>
</table>

References


