Information & Management 51 (2014) 69–79

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im

Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition

Princely Ifinedo

1250 Grand Lake Road, sydney, Canada

ARTICLE INFO

Article history:
Received 11 May 2011
Received in revised form 28 June 2013
Accepted 6 October 2013
Available online 18 October 2013

Keywords:
Information systems security policy
Behavioural intentions
Compliance
Socialisation
Social influence
Cognition

ABSTRACT

This study investigated employees' information systems security policy (ISSP) compliance behavioural intentions in organisations from the theoretical lenses of social bonding, social influence, and cognitive processing. Given that previous research on ISSP compliance has been based on deterrence theory, this study seeks to augment and diversify research on ISSP compliance through its theoretical perspective. Relevant hypotheses were developed to test the research conceptualisation. Data from a survey of business managers and IS professionals confirmed that social bonds that are formed at work largely influence attitudes towards compliance and subjective norms, with both constructs positively affecting employees' ISSP compliance. Employees' locus of control and capabilities and competence related to IS security issues also affect ISSP compliance behavioural intentions. Overall, the constructs in the research model enhance our understanding of the social-organisational and psychological factors that might encourage or accentuate employees' ISSP compliance in the workplace.

1. Introduction

To compete and survive in today's turbulent operating environments, organisations (public and private) continue to rely on and invest heavily in information systems (IS) [22,39]. The protection of the information and other data assets that are held in such systems is a major concern for practitioners and has emerged as a key managerial priority [13,28,33,51]. To protect critical IS assets, organisations often deploy security technologies, such as firewalls for perimeter defence and comprehensive monitoring systems (e.g., log management, data leak prevention, content monitoring technologies). These tools offer a technological or technical solution to the problem but are rarely sufficient in providing total protection of organisational IS resources [17,36,51]. This is because socio-organisational imperatives are considered relevant in fostering desired outcomes for organisations in such issues [36,42,45,52].

The onus is therefore on organisations to utilise multi-perspective approaches for protecting their IS assets and resources [17]. Researchers have indicated that organisations that fail to focus on individual and other organisational issues, alongside technology-based solutions, may fail to achieve success in their efforts [30,36,45,51,52]. Despite the huge investments that organisations make in procuring IS security tools, failings related to security incidents and breaches continue to be a significant problem [23,32,37]. One of the reasons why IS security incidents and abuses continue to plague organisations is that organisational employees are the weakest link in ensuring IS security; they constitute an insider threat to their organisations [13,42,45,52]. Thus, a beneficial approach to safeguarding IS resources requires that organisations focus on their own employees' intentions and behaviours.

One of the mechanisms that organisations use in shaping or influencing the behaviours of their employees with respect to how an IS is efficiently used is through the rules, guidelines, and requirements laid out in their information systems security policy (ISSP) [5,20,24,33,43]. However, the literature suggests that even if an ISSP is in place to help safeguard an organisation against the misuse, abuse, and destruction of IS assets, its employees often do not readily comply with such documents [13,23,33,51]. Studies are needed to enhance our understanding of issues that may serve to inhibit or encourage ISSP compliance in organisations. Research on ISSP compliance in organisations is beginning to receive increased attention in the extant literature [2,5,51–53].

Anderson and Agarwal's [2] review of the literature in this area indicated that the majority of previous ISSP compliance research was carried out from the perspectives of criminological theories (i.e., general deterrence theory, rational choice theory, situational crime prevention theory) and the health belief model (i.e., protection motivation theory). While previous research efforts favouring these perspectives have advanced knowledge in the area, we contend that other theoretical underpinnings could further provide insight into ISSP compliance. We argue that organisational

E-mail addresses: princely_ifinedo@cbu.ca, pifinedo@gmail.com.

0378-7206/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.im.2013.10.001

issues rooted in socialisation and social influence, as well as personal beliefs and cognition, can equally influence ISSP compliance behavioural intentions; others have provided similar arguments [5,15,17].

Research focusing on criminology has tended to accept sanctions and penalties as the only means by which IS misuse and abuse can be deterred [16,17,28,30]. Such studies implicitly have suggested that when violations and misbehaviours are severely punished, employees will cease to engage in such unacceptable behaviours. However, new insights have emerged that call this viewpoint into question. For instance, Vance et al. [51], Son [43], and Hu et al. [20] showed that ISSP compliance research using criminology and fear appeal theories do not always explicate noncompliance behaviours. According to these researchers, when employees err, they may use neutralisation techniques to circumvent or minimise the effects of reprisals from their organisations.

To increase knowledge, this research was designed to complement the few evolving studies based on socialisation and social psychology theories in understanding ISSP compliance in organisations [2,7,13,15,27]. Compliance, being a complex concept, should be studied from differing perspectives to enhance knowledge [3]. That said, it is axiomatic among scholars across disciplines that the Theory of Planned Behaviour (TPB), which encompasses Social Cognitive Theory (SCT), can explain innumerable behaviours, including ISSP compliance-related behaviours [15,27]. In this study, we integrated the recomposed TPB with Social Bond Theory (SBT), given that the latter may be suitable for adapting the former to working environments where social bonds might influence job-related perceptions and behaviours [7,13].

2. Theoretical background

2.1. Theory of planned behaviour

Social influence refers to the change in an individual's thoughts, actions, feelings, attitudes, or behaviours that results from their interactions with another individual or group [1,12]. The Theory of Reasoned Action, from which the theory of planned behaviour (TPB) was developed, underscores the social influence perspective. The TPB, which was proposed by Ajzen [1], postulates that individual behaviour is influenced by attitude, subjective norms, and perceived behavioural control. Attitude is defined as the individual's positive or negative feelings towards engaging in a specified behaviour. Subjective norms describe an individual's perception of what people important to them think about a given behaviour. Perceived behavioural control is defined as the individual's beliefs regarding the efficacy and resources needed to facilitate a behaviour.

The TPB has been widely used in investigating information system's ethical behaviours and individual's decision to comply with an ISSP [15,26,29]. Consistent with such previous studies, we posit that employees' intentions to comply with an ISSP will be influenced by attitude, subjective norms, and perceived behavioural control. However, we recomposed the TPB's perceived behavioural control construct by two measures related to social cognitive theory (SCT) for parsimony's sake and because the recomposed TPB tends to possess higher explanatory power [47]. The approach used here is consistent with those of others investigating comparable themes [54].

2.2. Social cognitive theory

Social cognitive theory is a relevant premise for explaining human behaviour [4]. SCT allows for the simultaneous and dynamic interplay between social and personal factors to be studied. SCT posits that individuals are actively engaged in their own development and obtain desired results when they believe that their actions are under their own control [4]. Accordingly, Workman et al. [54] decomposed SCT into two main elements; i.e., locus of control [40] and self-efficacy [4].

Locus of control refers to the degree to which an individual believes that he or she has the ability to control events that directly or indirectly affect them. Rotter [40] suggested that people who believe that they control their own destinies will accept responsibility for their actions. Essentially, people who feel that outcomes are beyond their control may shift the responsibility of their actions to others [40].

Self-efficacy simply refers to individuals' belief in their own competence and capabilities [4]. It fundamentally highlights the extent to which individuals feel and think about motivating themselves to completing specific tasks or actions. Stajkovic and Luthans [44] noted that such beliefs could cause individuals to think either pessimistically or optimistically regarding accomplishing work-related tasks. Similar to prior research [54] that used self-efficacy and locus of control to investigate computer safety behaviours, we posit that ISSP compliance will be positively enhanced when employees believe that they have the required competency and control to help them comply with their organisation's ISSP.

2.3. Social bond theory

Social bond theory (SBT) describes the binding ties or social bonding that individuals have with their group [19]. Hirschi [19] presented four bonds by which socialisation and conformity are promoted; i.e., attachment, commitment, involvement, and personal norms. The theory postulates that when people build upon such bonds, their urge to indulge in antisocial or antiestablishment behaviours is reduced. In the context of this research, attachment refers to the identification with organisational values vis-à-vis ISSP. Commitment highlights individuals' effort and energy expended to support their organisation's ISSP. Involvement refers to building relationships with other employees. Personal norms refer to an individual's own values and views of ISSP.

3. Research model and hypotheses

Following the preceding discussion, the research model is presented in Fig. 1. The decision to model the effects of SBT's constructs on attitude towards compliance and subjective norms is consistent with similar research conceptualisations in the area [2,5]. For instance, the TPB suggests that normative beliefs determine subjective norms, i.e., social influence or pressure. That is, if people believed that their referent individuals or groups (i.e., supervisors, coworkers) approved the behaviour, they would feel socially pressed to behave as expected. SBT's constructs explicitly measure social bonding in organisations and are closely related to subjective norms. In addition, attitude towards compliance benefits significantly from social information and interactions in the workplace [39,49]; thus, where greater bonding exists, favourable personal attitudes towards what a workgroup or an organisation considers important often ensue [7,13,15,46]. The control variables are included to enhance the insight into ISSP compliance. In particular, given the popularity of sanctions and penalties, i.e., deterrence theory, among IS security researchers [20,28,30,43], we decided to include constructs from that theory as part of the control variables. The research hypotheses are discussed next.

Employees attached to their organisations and with strong ties to colleagues tend to uphold values of importance to their organisations [6,39,46,49]. Chan et al. [7] found that employees

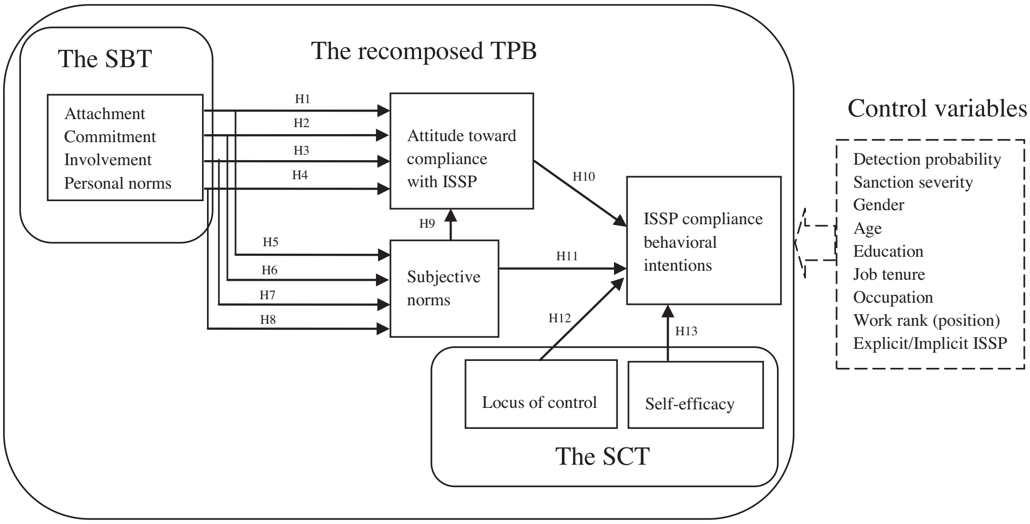

Fig. 1. The research model.

who socialise with colleagues with respect to ISSP compliance behaviours and issues in the workplace have higher perceptions of IS security in general. Similarly, Herath and Rao [16] provided empirical evidence to support the view that social influence plays a role in shaping employee security behaviours. Knapp and Marshall [24] implied that individuals can be persuaded to adhere to organisational ISSPs if they fear their attachment to colleagues may suffer from their noncompliance with such policies. Thus, attitudes towards ISSP compliance are favourably affected when individuals socialise with their colleagues with respect to their organisation's ISSP. Hence, the following hypothesis is proposed:

Hypothesis 1. Attachment will have a positive effect on attitude towards ISSP compliance.

Porter et al. [35] characterised organisational commitment as a strong belief in and acceptance of an organisation's goals and values, a willingness to exert effort on behalf of the organisation, and a strong desire to maintain membership in the organisation. Accordingly, an employee with strong beliefs in their organisation's values and goals, including those related to ISSP issues will form and maintain positive attitudes about the importance of such rules and guidelines. Recent studies show that employees are less likely to engage in counterproductive IS behaviours that may compromise their organisations' IS resources if their own commitment to the organisation is high [31,45,46,52]. Hence, the following hypothesis is proposed:

Hypothesis 2. Commitment will have a positive effect on attitude towards ISSP compliance.

Involvement simply means participation and engagement. Experts, including Thornton [50], have indicated that employees' involvement in their originations' activities, policies, and intentions boded well for the long-term success of businesses. In the context of this study, we posit that when individuals participate in meetings focusing on their organisation's ISSP and engage in personal relationships with colleagues in such matters, their attitudes towards complying with their organisation's ISSP will benefit accordingly. A study of computer abuse behaviours by Lee et al. [26] that used similar measures as this current study showed that employees' involvement positively affected intentions and attitudes towards engagement in desired behaviours. Hence, the following hypothesis is proposed:

Hypothesis 3. Involvement will have a positive effect on Attitude towards ISSP compliance.

Personal norms, standards, benefits, and values matter in how an employee perceives organisational issues, including those relating to the adherence of acceptable computer behaviours [30]. In general, the literature has shown that personal norms have a bearing on an individual's attitude towards engaging in computer abuse and organisational IS misbehaviour [2,26,27,30,32]. It is to be expected that employees with favourable personal values and norms will form positive attitudes towards complying with their organisation's ISSP. Indeed, researchers have confirmed that personal norms, benefits and values positively influence attitudes towards engaging in and complying with acceptable computer security behaviours and guidelines [7,32,53,54]. Hence, the following hypothesis is proposed:

Hypothesis 4. Personal norms will have a positive effect on attitude towards ISSP compliance.

As with the foregoing discussions about the impacts of SBT's constructs (i.e., Attachment, Commitment, Involvement and Personal norms) on Attitude towards compliance, we believe that similar arguments would hold for the relationships between these constructs and Subjective norms. For instance, a committed, involved worker with acceptable personal values and, having strong attachment to his or her organisational objectives, will find it agreeable and expedient to follow cues from significant others in his or her work environment [6,39,49]. Indeed, workers' perceptions of organisation-wide issues, e.g., ISSP compliance, can be linked with or influenced by the viewpoints of their referent individuals or groups (i.e., supervisors, coworkers) [7,15,16,23]. Recent research has shown that workgroup's opinions and concerns have a bearing on ISSP compliance in the workplace [13,23]. As previously noted, Knapp and Marshall [24] found that workers may be persuaded to follow directives in their organisation's ISSP if noncompliance is perceived to arise from weak attachment. In addition, it has been shown that employees sharing a similar level of commitment as their colleagues are less likely to engage in counterproductive behaviours if their colleagues and peers are not engaged in such [16–18,31,39,49]. Workers who are involved with their organisation is likely to comply with their group's acceptable engagements and behaviours [7,17,24,50]. When an employee bonds with peers in the workplace, it is likely that his or her personal norms and values will not depart from those of his or her referent individuals or groups [39]. Hence, the following hypotheses are proposed:

Hypothesis 5. Attachment will have a positive effect on Subjective norms.

Hypothesis 6. Commitment will have a positive effect on Subjective norms.

Hypothesis 7. Involvement will have a positive effect on Subjective norms.

Hypothesis 8. Personal norms will have a positive effect on Subjective norms.

In general, the attitudes that people have about an issue or act can be influenced by the views of significant others [1,12]. Thus, an employee's attitude about ISSP compliance at his or her organisation can be influenced by the pervading views of referent individuals or groups [7,13,15,23]. Thus, where the group's view of an issue is favourable, the individual's attitude may follow suit. In the context of IS security behaviour, Chan et al. [7], Guo et al. [13], Hazari et al. [15], Ifinedo [23], and Herath and Rao [17] found that subjective norms positively affect attitude towards compliance. Hence, the following hypothesis is proposed:

Hypothesis 9. Subjective norms will have a positive effect on Attitude towards ISSP compliance.

Conceptually, the TPB posits that positive attitudes influence behavioural intentions. Conversely, negative attitudes will diminish behavioural intentions. Thus, employees with positive beliefs about their organisation's ISSP will have favourable tendencies to comply with such rules and guidelines [32,42]. On the other hand, those lacking such favourable attitudes will not readily comply with such policies. Other studies have shown that attitudes towards complying with acceptable IS behaviours positively affect behavioural intentions [2,5,33]. Hence, the following hypothesis is proposed:

Hypothesis 10. Attitude towards ISSP compliance will have a positive effect on ISSP compliance behavioural intentions.

Essentially, subjective norms are normative stimuli, beliefs and motivations related to compliance with a particular act, which is largely informed by consultation or observation of the behaviours of others [1,3,12]. Indeed, individuals' behaviour is influenced or motivated by what they observe to be normal in their environment [7,24]. In the context of ISSP compliance in organisations, employees are most likely to comply with their organisation's ISSP if they notice that those around them, i.e., superiors, peers, and subordinates, are complying with and abiding by such guidelines [7,17]. Pahnila et al. [33], Bulgurcu et al. [5] and Herath and Rao [16] found that subjective norms significantly affect ISSP compliance in organisations. Hence, the following hypothesis is proposed:

Hypothesis 11. Subjective norms will have a positive effect on ISSP compliance behavioural intentions.

Locus of control relates to individuals' control over events affecting them. Thus, employees who perceive to have control over issues affecting them or others tend to assume responsibility for their actions. In the context of engaging in precautionary IS measures, it has been shown that individuals with higher control perceptions are more proactive in terms of undertaking higher security precautions, such as installing and updating security and virus software, changing passwords at regular intervals, and using firewalls and backup systems [41,54]. Thus, employees' locus of control will have significant influence on their ISSP compliance behavioural intentions. Workman et al. [54] found locus of control to be positively related to IS security behaviours. Hence, the following hypothesis is proposed:

Hypothesis 12. Locus of control will have a positive effect on ISSP compliance behavioural intentions.

Self-efficacy relates to individuals' capabilities and competence to cope with a task or make a choice [4]. In particular, self-efficacy has been shown to have a significant impact on an individual's ability to accomplish tasks, including IS usage [10]. Compeau and Higgins [10] showed that people with higher self-efficacy regarding IS use are more likely to employ such systems in their work more than those with low self-efficacy. With respect to ISSP, it is logical to expect that individuals with high IS security capabilities and competence will see the need to follow organisational ISSPs and that such individuals will be better able to understand the dangers of noncompliance. Recent findings have confirmed that ISSP compliance is positively affected by self-efficacy [5,16,23,33,43,54]. Hence, the following hypothesis is proposed:

Hypothesis 13. Self-efficacy will have a positive effect on ISSP compliance behavioural intentions.

4. Research methodology

4.1. Data collection procedure

The research model was tested using a field survey. To that end, we used two approaches in collecting our data. First, we purchased a directory containing the names of non-IS managers in Canadian organisations from a marketing and data research firm, i.e., InfoCanada. Half of the names on the list, which constituted 1000 names, were used for this study. Each participant received a cover letter, questionnaire, and self-addressed, stamped envelope. Of the 1000 questionnaires that were mailed, 106 were undelivered. In all, 76 responses were received, reflecting an effective response rate of 8.5% from this particular source. Excluding 8 incomplete and poorly completed responses, we were left with 68 responses from this source. The response rate is relatively high in light of the difficulties of collecting security-related data from organisations [25].

Second, in order to increase our knowledge of ISSPs in organisations, the views of IS professionals were also obtained [5,16,22,23,28]. As we were unable to procure a list of IS professionals in Canada, we decided to use judgmental sampling [21] to collect data from such professionals. In this approach, a researcher uses their judgement to select suitable participants. We contacted the chapter heads of the Information Systems Audit and Control Association (ISACA) across Canada, who we asked to direct their members to an online version of the same questionnaire that was mailed to non-IS managers (the survey was hosted by QuestionPro.com). Additionally, we used contacts to solicit participation from other IS professionals across the country. Fifty-six (56) usable responses were obtained from IS security and other IS professionals.

Both cohorts were motivated by four $100 gift certificates and a promise to share the summary of the results with them. Importantly, participation in the study was voluntary, and the respondents were assured that individual responses would be treated with anonymity and confidentiality. These incentives were necessary as it is known that individuals (and organisations) are hesitant to participate in security-related surveys [25]. Thus, a total of 124 usable responses from both groups are considered adequate for an exploratory study such as this one. It is worth noting that our data sample size is comparable with those of similar studies in the literature [7,23,32].

As the unit of analysis was the individual employee, common method variance (CMV) was not a problem for the study. Nonetheless, procedural remedies for controlling CMV bias were followed. Namely, clear and concise questions were used in the questionnaire, and as indicated above, to reduce apprehension, respondents' anonymity was assured. Additionally, a statistical procedure, i.e., the Harmon one-factor test, was used to assess whether such biases were indeed a problem in our sample [34]. The test results showed that several factors with eigenvalues greater than one were present in our data. The most covariance explained by one factor was our data is 24.6%, indicating that CMV was not a problem in the data.

We compared early and late respondents from both the mail and the online survey to assess whether non-response bias existed in our data, [21]. The independent *t*-test did not show any statistically differences between the survey's non-participants (late respondents) and participants (early respondents) regarding the characteristics of age, gender, education, job tenure at their current place of work, and occupation.

On average, the study's respondents had 10.14 years (s.d. = 9.4) of tenure at their current organisations. Some of the job title of the IS professionals included IS Directors, Chief Information Security Officers, and IS Project managers. Of the non-IS managers, job title included Chief Human Resources Officers, VPs of Marketing, and Accounts Managers. There were 68 (55%) non-IS managers and 56 (45%) IS professionals in the sample. Table 1 shows the job rankings (positions) and other demographic information for the respondents.

Table 1
Demographic characteristics of the sample (N = 124).

Variable	Frequency	Percent (%)
Gender		
Male	73	58.9
Female	51	41.1
Age range		
21–30 years	24	19.4
31–40 years	28	22.6
41–50 years	34	27.4
50–60 years	30	24.2
61 years and above	8	6.5
Educational attainment		
Secondary education	14	11.3
Vocational/technical	21	16.9
University education	85	68.5
Missing	4	3.2
Rank (position)		
Top management personnel	28	22.6
Mid-level personnel	82	66.1
Junior staff	14	11.3
Industry		
Manufacturing	20	16.1
Retail/wholesale	8	6.5
Telecoms/IT	24	19.4
Finance/insurance	12	9.7
Healthcare	14	11.3
Education	10	8.1
Government	8	6.5
Transportation	4	3.2
Other (e.g. real estate, utility, forestry, hotel)	19	15.3
Missing	5	4
Annual revenue (CDN$)		
Less than $500,000	12	9.7
$500,001–$1 million	8	6.5
$1.1–$5 million	20	16.1
$5.1–$10 million	2	1.6
$10.1–$20 million	4	3.2
$20.1–$50 million	6	4.8
$50.1–$100 million	16	12.9
$100 million and above	42	33.9
Missing	14	11.3
Number of employees		
Under 10 people	8	6.5
11–250 people	38	30.6
251–500 people	19	15.3
501–1000 people	11	8.9
1001–5000 people	20	16.5
5001–10000 people	2	1.6
10,000 people and above	18	14.5
Missing	8	6.5
Availability of formal ISSP		
No	49	39.5
Yes	55	44.4
I don't know	13	10.5
Missing	7	5.6

4.2. Operationalisation of the constructs

The nine main constructs that were used in this study were taken from previously validated research; we adapted the measures to the ISSP compliance research context. The scales for attachment (ATCH) and involvement (INVO) were adapted from Lee et al. [26]. The scale for commitment (COMM) was adapted from Lee et al. [26] and Herath and Rao [16]. For the personal norms (PERN) scale, we adapted relevant measures from Li et al. [30]. The measures for the two constructs of attitude towards compliance with ISSPs (ATWB) and subjective norms (SUBN) were adapted from Woon and Kankanhalli [53], Bulgurcu et al. [5], and Herath and Rao [16,17]. We modified the measures from Workman et al. [54] for the locus of control (LOCC) scale.

Self-efficacy (SEFF) used measures adapted from Compeau and Higgins [10], Woon and Kankanhalli [53], and Workman et al. [54]. The behavioural intentions (BEHI) scale included measures modified from Woon and Kankanhalli [53] and Herath and Rao [16,17]. The measurement items were mainly 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 questionnaire was pre-tested by knowledgeable professionals including 4 IS faculty members, 8 local IS managers and 8 non-IS managers with some experience in ISSP issues. The measurement items, individual descriptive statistics and sources of the study's scales are provided in Appendix A. The deterrence control variable items [16,17] and scales are provided in Appendix B.

5. Data analysis and results

The partial least squares (PLS) technique of structural equation modelling, which uses a principle component-based estimation, was used for the analysis. The approach is suitable for validating predictive models, particularly those with small size samples [8]. The specific tool that was used was SmartPLS 2.0, which was created by Ringle et al. [38]. PLS supports two measurement models: (a) the assessment of the measurement model and (b) the assessment of the structural model.

5.1. Assessment of the measurement model

The psychometric properties of a model are examined by the following indicators: internal consistency, convergent validity, and discriminant validity. Hair et al. [14] suggested that item loadings of 0.5 are adequate for these indicators; items with values lower than 0.5 were thus deleted from the scales. The composite reliability for each of the study's constructs was above the recommended level of 0.7, indicating the internal consistency of the data [13]. Fornell and Larcker [11] recommended that the average variance extracted (AVE) criterion be used to assess convergent validity. These researchers suggested that an AVE value

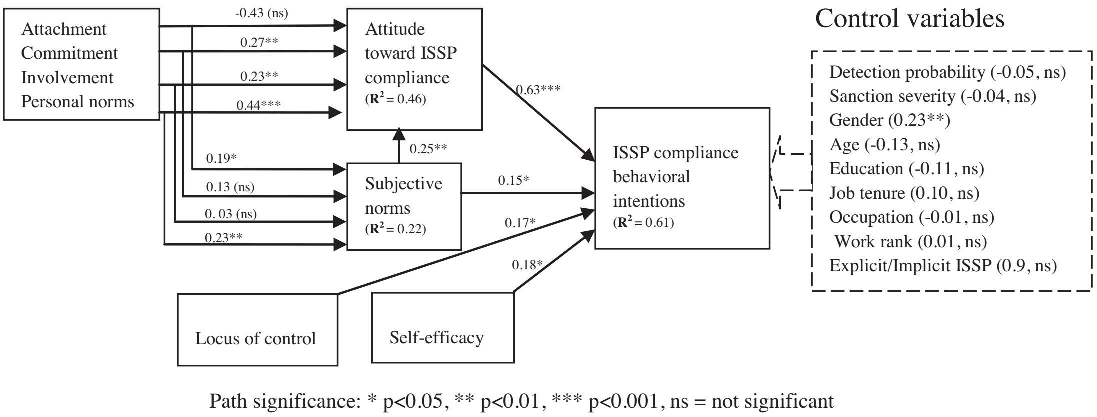

Fig. 2. The SmartPLS 2.0 results for the tested relationships. Path significance: $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$, ns = not significant.

Table 2
Descriptive statistics, construct reliabilities, AVEs, and inter-construct correlations.

Construct	Mean	SD	CR	AVE	Construct								
					1	2	3	4	5	6	7	8	9
1: ATCH	4.80	1.24	0.90	0.81	**0.90**								
2: COMM	6.20	0.77	0.85	0.59	0.57	**0.77**							
3: INVO	5.77	1.10	0.74	0.60	0.30	0.36	**0.77**						
4: PERN	5.76	1.26	0.81	0.59	0.57	0.56	0.25	**0.77**					
5: ATWC	6.33	0.75	0.97	0.90	0.20	0.46	0.31	0.53	**0.95**				
6: SUBN	5.72	1.09	0.84	0.64	0.39	0.37	0.20	0.41	0.42	**0.80**			
7: LOCC	4.61	1.47	0.69	0.57	0.20	0.19	0.14	0.37	0.10	0.24	**0.75**		
8: SEFF	4.86	1.58	0.86	0.62	0.23	0.09	−0.08	0.08	−0.01	0.10	0.35	**0.79**	
9: BEHI	6.16	0.90	0.90	0.70	0.28	0.48	0.30	0.54	0.70	0.46	0.33	0.24	**0.84**

Notes: (a) Composite reliability (CR), standard deviation (SD), average valance extracted (AVE), attachment (ATCH), commitment (COMM), involvement (INVO), personal norms (PERN), attitudes towards compliance (ATWC), subjective norms (SUBN), locus of control (LOCC), self-efficacy (SEFF), behavioural intentions (BEHI). (b) The bold fonts in the leading diagonals are the square root of AVEs. (c) Off-diagonal elements are correlations among constructs.

of 0.50 is acceptable, as it indicates that a latent variable is able to explain more than half of the variance of its indicators, on average. This study's AVE values were adequate, as shown in Table 2.

Discriminant validity is assured when the following two conditions are met: (a) the value of the AVE is above the threshold value of 0.50 and (b) the square root of the AVE is larger than all other cross-correlations. Table 2 shows that the AVE ranged from 0.57 to 0.90, and in no case was any correlation between the constructs greater than the squared root of AVE (the principal diagonal element). Overall, the results showed that the study measures were psychometrically adequate for this study (Table 2).

5.2. Assessment of the structural model

The structural model presents information about the path significance of hypothesised relationships using the path coefficients (β) and R squared (R^2). The strength of the relationship is indicated by the β. Chin [8] notes that R^2 values of 0.67, 0.33, and 0.19 for the percentage of variance in a model are substantial, moderate and weak, respectively. The R^2 shows the percentage of variance in the model to give an indication of its predictive power. The SmartPLS 2.0 results for the β and R^2 values are shown in Fig. 2 path significance levels (t-values) are estimated using the bootstrapping method. Additionally, Cohen [9] suggested that the PLS structural model can be assessed using effect sizes, f^2. Moreover, Tenenhaus et al. [48] noted that tests for the predictive relevance of a model can be gauged from its goodness-of-fit index (GoF) and Stone–Eiser q-square (q^2) indicators.

According to Cohen [11], f^2 values of 0.02, 0.15, and 0.35 signify small, medium, and large effects, respectively. The goodness-of-fit (GoF), which is the geometric mean of the average communality (outer measurement model) and the average R^2 of endogenous latent variables, is used to assess the overall fit of a model. The GoF validates a PLS model by presenting a compromise between the performance of the measurement and the structural model; it is normalised between 0 and 1, where a high value indicates better path model estimation. The q^2 statistic measures the predictive relevance of the model. A q^2 greater than 0 indicates that a model has predictive relevance, and values less than 0 indicate a lack of predictive relevance. Table 3 presents the β, R^2, GoF, t-values, f^2, and q^2 for the research model. The results obtained in this study indicate that the research model is structurally sound, as it possesses adequate predictive relevance and performance.

Fig. 2 and Table 3 show the structural model's results. Three out of the four hypotheses relating SBT's constructs to attitude towards compliance were supported, the exception being Hypothesis 1.

Table 3
Relevant indicators for the structural model.

Path	β	t-value	f^2
Attachment → attitude	−0.43	3.612	0.18
Commitment → attitude	0.27	2.728	0.08
Involvement → attitude	0.23	1.882	0.07
Personal norms → attitude	0.44	3.661	0.21
Attachment → subjective norms	0.19	1.730	0.24
Commitment → subjective norms	0.13	1.091	0.01
Involvement → subjective norms	0.03	0.249	0.00
Personal norms → subjective norms	0.23	1.716	0.04
Subjective norms → attitude	0.25	2.295	0.11
Attitude → behavioural intentions	0.63	8.850	0.81
Subjective norms → behavioural intentions	0.15	1.948	0.04
Locus of control → behavioural intentions	0.17	1.638	0.05
Self-efficacy → behavioural intentions	0.18	1.903	0.07

The R^2 of the research model is 0.61.
The GoF for the research model is 0.40.
The q^2 of the research model is 0.42.

Half of the hypotheses relating SBT's constructs to subjective norms were supported; namely, H6 and H7 were unconfirmed. Obviously, the formulated hypotheses were largely supported by the results.

Contrary to the stated prediction, the data did not support H1, i.e., the impact of attachment on attitude towards compliance ($\beta = -0.43$, t-value = 3.601). The obtained result is statistically significant at the $p < 0.01$ level; however, it cannot be accepted due to its negative direction. Nevertheless, this result appears to suggest that it is possible for an employee to have a positive attitude about his or her organisation's ISSP yet hold differing perceptions from coworkers. According to Casper and Harris [6], perceived individual benefits and self-interest are some of the possible causes of such discord.

It is somewhat surprising that H6 (Commitment will have a positive effect on Subjective norms) and H7 (Involvement will have a positive effect on Subjective norms) were unsupported. It is difficult to make sense of these findings; however, a plausible explanation for these results might involve the scale composition, research sample, or other extraneous influences. For instance, a perceived lack of involvement and/or rift between IS professionals and business managers vis-à-vis organisational IS issues has been reported [22].

H2–H4 were supported, indicating that Commitment, Involvement, and Personal norms have positive effects on Attitude towards compliance with ISSP. These three factors, together with Attachment and Subjective norms, jointly explained 46% of the variance in Attitude towards compliance. These results are consistent with postulations in SBT indicating that socially involved and committed individuals with appropriate personal values who benefit from the influence of significant others will develop acceptable attitudes that will ultimately shape their attitudes towards a behaviour, in this instance ISSP compliance [7,15,17,23,26].

Support for H5 confirmed that employees tend to be more bonded with colleagues' views of their organisation's ISSP when they are strongly attached to their organisational objectives in such matters [7,39,49]. Similarly, our data analysis confirmed H8, suggesting that Personal norms are positively related to Subjective norms [7,17,39]. The four SBT's constructs explained 22% of the variance in Subjective norms. Support for H9 was also provided, affirming the prediction indicating that employees' Attitude towards compliance would strongly benefit from the influence of significant others [7,13,15,17,27,39].

H10, which predicted that Attitude towards compliance with ISSPs would have a positive effect on ISSP compliance behavioural intentions, was confirmed. Attitude towards compliance has the largest effect size on ISSP compliance behavioural intentions. This finding is consistent with the results of other studies based on the TPB [15,27]. The hypothesised, positive impact of Subjective norms on ISSP compliance behavioural intentions (H11) was also supported by the data. This result is in agreement with the findings of others [5,7,13,15,17,27]. H12 was confirmed, supporting the notion that an individual's locus of control is crucial in encouraging ISSP compliance behavioural intentions. Moreover, the data analysis supported H13, which predicted that individual's self-efficacy would have a positive effect on ISSP compliance behavioural intentions. The findings regarding the pertinence of both the individual's locus of control and self-efficacy in the research model are consistent with the tenets of both SCT and TPB and mirror results from comparable studies [5,16,23,33,43,54].

All the study's variables explain 61% of the variance in the dependent construct. This result suggests that the amount variance explained by the study's variables is between moderate and substantial [10], therefore contributing to our understanding of ISSP compliance. Regarding the control variables, only gender was found to have a significant effect on the dependent variable. Namely, male (mean = 6.04, s.d. = 0.875) and female (6.14, s.d. = 0.789) respondents had differing ISSP compliance behavioural intentions [16,28].

6. Discussions

6.1. Research contributions and implications

This study offers several contributions to the IS security management literature. To the best of our knowledge, it is among the first studies to integrate the theory of planned behaviour – which encompasses social cognitive theory – with social bond theory for use in IS security discourse. This integrative conceptualisation offers a new perspective in understanding employees' ISSP compliance behavioural intentions, which we believe supplements research based on other, widely publicised theoretical lenses, such as deterrence theory and protection motivation theory. Furthermore, this research supports the postulations in SBT, SCT, and the TPB in so far as perceptions of social norms, group influence, and cognitive abilities can serve to discourage or curtail unacceptable behaviours with respect to ISSP compliance.

The suitability of the TPB – either the overarching theory or its extensions – for IS security behaviours is strongly supported by our data. In fact, a quick scan of the literature shows that studies using some of the other theoretical perspectives have found that the variance explained (R^2) by the antecedents of ISSP compliance is about 40%. For example, Vance et al. [51], Son [43], and Herath and Rao [17] reported R^2 values of 0.44, 0.42, and 0.42, respectively. On the other hand, studies based on the TPB tend to have higher explanatory power; please see, for example, Hazari et al. [15], Lee and Kozar [27], and this current effort, with R^2 values of 0.58, 0.55, and 0.61, respectively. It is safe to suggest that the understanding of ISSP compliance may be deepened by integrating the TPB with other perspectives.

It does not appear that a worker's decision to comply with his or her organisation's ISSP largely depends on perceived sanctions and penalties [16,17,28,30]. To a lesser degree, the data analysis of this current research seems to lend credence to an emerging viewpoint in the literature [13,20,43,51], showing that the use of deterrence theory as an overriding means by which employee's ISSP compliance/noncompliance can be explicated may require further re-examination. It is safe to suggest that this study complements previous findings by integrating social components as factors influencing employees' intention to comply with ISSP. Social factors have not been considered in studies based on deterrence theory.

This study furthers our understanding of ISSP compliance by demonstrating the pertinence of the effects of socialisation, influence and cognition on ISSP compliance behavioural intentions. We argued and found support for the hypothesis suggesting that employees form social bonds at work and that they may use significant others as role models for analysing the appropriateness of particular beliefs and behaviours [7,13,15,17,39,49]. Such bonds influence their attitude towards compliance, which augurs well for behavioural compliance, in this instance for ISSP compliance. We confirmed that when an employee has perceives to have control over issues affecting them or others in their workplace, they may readily assume responsibility for their actions, i.e., ISSP compliance. In addition, with adequate capabilities and competence to cope with IS security issues, an employee will make a choice to comply with his or her organisation's ISSP [23,43,54]. The IS security management literature is augmented by such findings.

By including the views of both IS professionals and non-IS managers, this research broadens knowledge regarding IS security behaviours in organisations from the viewpoint of both cohorts.

Such considerations are necessary for enhancing insight into ISSP compliance [16,22,26,30]. This study provides a testable research conceptualisation that other studies can further develop. One possible area of interest might be to use the constructs in this study and other perspectives in the extant literature to develop a comprehensive, integrative contingency model for assessing ISSP compliance in organisations. An extension to this current effort could investigate the effects of organisational citizenship behaviours (OCB) and social and organisational learning perspectives on ISSP compliance. Additionally, given that Personal norms were found to be the most influential bonding element on Attitude towards compliance and Subjective norms, future research could examine how Personal norms vis-à-vis IS security issues in the workplace could be further enhanced.

6.2. Implications for practice

This study suggests that management can increase ISSP compliance by providing an environment where individuals can learn organisational values and the importance of their organisation's ISSP through co-worker socialisation. Organisation-wide relationships focusing on inter- and intra-unit levels with respect to ISSP issues may serve to encourage group conformity with organisational IS rules and requirements. Put differently, individuals are more likely to buy in to their organisation's ISSP when they know that complying with the ISSP is a *social issue* that benefits their colleagues and others in the organisation. By the same token, influential people in organisations who are capable of motivating or shaping the opinions of others could be tasked to *champion* the cause of ISSP compliance. Overall, individual attitudes towards ISSP compliance are positively enhanced by such input.

In the context of this research, the results showing a lack of support for the impact of Attachment, Commitment and Involvement on Attitude towards compliance and Subjective norms raise an interesting question. Perhaps ensuring that all employees sing from the same hymn book with respect to organisational IS security is the best way forward; however, such may be difficult to achieve due to individual self-interests. Nevertheless, whenever possible, management should promote and encourage organisational bonding with respect to IS security concerns. Regular group meetings on such matters may be one means of doing so. Complete adherence to social norms and values in any organisation requires an extensive socialisation process [39,49]; where such socialisation is achieved, favourable outcomes regarding ISSP compliance may ensue [7,13,23].

As the bonding element of Personal norms has the most significant impact on Attitude towards compliance and Subjective norms, management should ensure that employees with negative personal beliefs about IS security issues are provided greater education and awareness regarding such matters [20], and proactive efforts should be made to socialise or 'bond' lagging individuals with peers who are already familiar with the organisation's values and objectives. Indeed, workers learn important values and cues from coworkers and superiors [49]. In addition, rewards and incentives aimed at improving personal beliefs about IS security issues could be used.

Given the significant effects of Attitude towards compliance, Locus of control, and Self-efficacy on ISSP compliance behavioural intentions, management may consider adopting the following strategies: (1) Management could strive to provide regular in-house IS security awareness sessions, campaigns and training to positively shape the normative beliefs and, eventually, the attitudes of their workers regarding IS security issues and concerns. Those lacking proper attitudes related to their organisation's ISSP and related guidelines could benefit from such regular orientation and education. (2) IS security procedures, practices, and directives should not be intimidating and cumbersome, so as to not discourage ordinary workers from attempting to assume responsibility for basic IS security matters. When workers perceive to have control over such issues, they tend to comply with policies related to such issues, in this instance ISSP. (3) There is a need to provide facilitating conditions, such as general exposure to emerging security technologies and relevant incentives to encourage individuals to take it upon themselves to develop or improve the necessary skills and knowledge that are required to help safeguard organisational IS assets. The availability of such encouragement in relation to skill acquisition will facilitate employees' ISSP compliance. (4) Practitioners should also pay attention to gender differences in relation to ISSP compliance in organisations. This research suggests that males appeared to have lower compliance intentions compared to their female counterparts. Targeted awareness programmes and monitoring are examples of measures that could be used to bridge apparent gaps in behaviour between genders.

6.3. Limitations of the study

There are limitations to this study. Although common method bias was not a problem for this study, it is still possible that the participants provided socially desirable responses [32] to some of the issues being investigated. Moreover, the sample is not entirely random, which might negatively affect the generalisability of the study's findings. The sample was based on 124 responses. Although the research conceptualisation and analysis met the requirements for using the PLS technique [8], a larger sample size may provide more statistical power and performance.

The study included the views of respondents who have formal ISSPs in their organisations and those who do not. The inclusion of both types of respondents might have negatively affected the results. Nonetheless, the questionnaire that was used provided the participants with clear information about the study (please see Appendix B). Further, comparisons of the groups' responses did not show significant, statistical differences between the two groups. The data were obtained from a cross-sectional field survey; longitudinal data may provide more insight into ISSP compliance. Future research in this area may consider using qualitative approaches, including action research and focus groups, to provide further insight into ISSP compliance.

7. Conclusions

Prior research on ISSP compliance and computer security behaviours in organisations has adopted the perspectives of criminological theories and health belief theory. While such perspectives are important, we argue that the literature can benefit from other relevant theoretical underpinnings. To that end, we proposed and empirically tested a research model that drew from the influences of socialisation, group influences, personal beliefs, self-efficacy, and cognition. Our findings showed that the proposed factors indeed affect ISSP compliance in organisations. To a large degree, the study's results indicated that socio-organisational factors affect individuals' attitudes towards ISSP compliance and subjective norms, which in turn affect ISSP compliance behavioural intentions. In addition, social influence and individuals' perceptions of their control and competence with regard to IS security issues have a positive effect on ISSP compliance behaviours. By focusing on the constructs considered in this study, knowledge of ISSP compliance is augmented and diversified.

Acknowledgements

This research project was sponsored by a grant (ORAI – #8271) provided by Cape Breton University, Canada. I am grateful to C. M. Ringle, S. Wende, and A. Will for the use of their software, SmartPLS 2.0. Special thanks go to all the study's participants and the project's Research Assistants: Lindsay McDonald and Cindy Butler. I appreciate the comments and suggestions provided by anonymous reviewers of earlier drafts of this paper.

Appendix A

The questionnaire's items, their descriptive statistics, item loadings, and constructs' sources.

Construct	Item	Mean	S.D.	Loading (*t*-value)	Source
Attachment	I usually have conversations about my organization's ISSP with close co-workers	3.92	1.77	0.860 (12.706)	[23]
	I respect my co-workers' views and opinions about our organization's ISSP	5.32	1.23	0.538 (3.722)	
	I communicate the importance of the organization's ISSP to co-workers	5.13	1.64	0.909 (19.606)	
Commitment	I strongly believe that my organization's ISSP can help the organization to succeed	6.14	0.91	0.746 (11.751)	[23,16]
	I am committed to promoting my organization's ISSP	6.13	0.75	0.860 (22.069)	
	I am willing to invest energy and effort in making the organization's ISSP a success	6.18	0.68	0.874 (23.841)	
	I am willing to put in a great deal of effort to help my organization succeed	6.34	0.72	0.554 (6.109)	
Involvement	I value the opportunity to participate in informal meetings related to my organization's information security	5.08	1.51	0.539 (2.271)	[23]
	I work on building personal relationships with many co-workers in my organization vis-à-vis ISSP concerns	5.65	1.28	0.557 (2.967)	
	I actively involve myself in activities related to my organization's growth	5.89	0.92	0.855 (6.191)	
Personal norms	It is serious matter if I don't comply with my organization's ISSP	5.81	1.40	0.464[a] (1.295)	[27]
	It is unacceptable to not follow ALL guidelines and measures outlined in the organization's ISSP	5.77	1.28	0.716 (5.625)	
	To me, following the organization's ISSP is NOT a trivial offence	5.51	1.39	0.713 (6.363)	
	To me, it is unacceptable to ignore my organization's ISSP measures and guidelines	6.03	1.10	0.870 (17.499)	
Attitude toward ISSP compliance	Following the organization's ISSP is a good idea	6.32	0.74	0.830 (34.408)	[6,49]
	Following the organization's ISSP is a necessity	6.27	0.79	0.940 (66.071)	
	Following the organization's ISSP is beneficial	6.40	0.71	0.982 (219.463)	
	Following the organization's ISSP is pleasant	5.85	1.25	0.009[a] (0.015)	
Subjective norms	My boss thinks that I should follow the organization's ISSP	5.86	0.97	0.684 (7.466)	[6,16,17,49]
	My colleagues think that I should follow the organization's ISSP	5.73	1.11	0.887 (31.428)	
	My subordinates think I should follow the organization's ISSP	5.57	1.20	0.818 (15.765)	
Locus of control	I believe that it is within my control to protect myself from information security violations	5.66	1.16	0.986 (11.705)	[50]
	The primary responsibility for protecting my organization's information belongs to others and not me	2.98	1.74	−0.761[a] (1.424)	
	Keeping my organization's information safe[b]	5.19	1.51	0.506 (2.003)	
Self-efficacy	I have the necessary skills to protect myself from information security violations	5.08	1.55	0.942 (3.628)	[12,49,50]
	I have the expertise to implement preventative measures to stop people from getting my confidential information	4.81	1.60	0.885 (3.454)	
	I have the skills to implement preventative measures to stop people from damaging my work computer	5.15	1.35	0.768 (3.027)	
	It is easy for me to enable security features on my work computer by myself	4.39	1.82	0.559 (2.372)	
	I can enable security measures on my work computer but only when I have manuals for reference	3.32	1.64	−0.428[a] (0.563)	
	For me, taking information security precautions[c]	4.16	1.79	0.371[a] (1.413)	
	My ability to prevent information security violations at my workplace[d]	4.10	1.77	0.360[a] (1.369)	
ISSP compliance behavioral intentions	It is my intention to continue to comply with the organization's ISSP	6.34	0.72	0.818 (10.717)	[6,17,49]
	I am certain I will adhere to my organization's ISSP	6.15	0.81	0.819 (12.470)	
	I am likely to follow the organization's ISSP in the future	6.13	1.01	0.859 (25.669)	
	I would follow the organization's security policy whenever possible	6.02	1.09	0.855 (28.292)	

[a] These items were deleted from further data analysis due to their low item loadings.

[b] These items were assessed by the following parameters: Beyond my control (1) . . .Within my control (7).

[c] These items were assessed by the following parameters: Hard (1). . .Easy (7).

[d] These items were assessed by the following parameters: Inadequate (1). . . Adequate (7).Appendix BItems used to operationalize the control variables of detection probability and sanction severity and the definition of ISSP provided to the study's participants.

Variable	Item	Scale	Source
Detection probability	The probability that I would be caught if I failed to comply with my organization's IS security policy is:	Very low = 1... Neutral = 4... Very high = 7	[16,17]
	I can easily bypass my organization's IS security policy guidelines without being caught:	Strongly disagree = 1... Neutral = 4... Strongly agree	
Sanction severity	If I were caught not adhering to my organization's IS security policy directives, I think the punishment would be:	Not very serious ... Neutral =4...Very serious = 7	
	If I were caught not adhering to my organization's IS security policy directives, I would be severely punished by my organization:	Strongly disagree = 1... Neutral = 4... Strongly agree = 7	

Definition of ISSP provided to the study's participants

A formal organization IS policy is typically a document that outlines specific requirements or rules that must be met to safeguard organizational IS assets from intention abuse or destruction. It is formal when it is EXPLICITLY defined or stated.

Organizational IS policies sometimes are IMPLICITLY stated in other organization's rules and procedures. For the purposes of this study, participants who don't have a formal organization IS policy could think of "acceptable" policies and practices in their organizations related to the following: information access control, downloading illegal software and freeware, using anti-spyware, anti-virus tools and firewalls, responding to spam emails, changing passwords at intervals, visiting suspicious websites, storing sensitive information on unsecured computers, backing up systems, and so forth.

References

[1] I. Ajzen, The theory of planned behavior, Organizational Behavior and Human Decision Processes 50 (2), 1991, pp. 179–211.

[2] C.L. Anderson, R. Agarwal, Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions, MIS Quarterly 34 (3), 2010, pp. 613–643.

[3] E. Aronson, D.W. Timothy, R.M. Akert, Social Psychology, Prentice Hall, Upper Saddle River, NJ, 2010 p. 2010.

[4] A. Bandura, Self-Efficacy: toward a unifying theory of behavioral change, Psychological Review 84 (2), 1977, pp. 191–215.

[5] B. Bulgurcu, H. Cavusoglu, I.I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS Quarterly 34 (3), 2010, pp. 523–548.

[6] W.J. Casper, C.M. Harris, Work-life benefits and organizational attachment: Self-interest utility and signaling theory models, Journal of Vocational Behavior 72 (1), 2007, pp. 95–109.

[7] M. Chan, I.M.Y. Woon, A. Kankanhalli, Perceptions of information security at the workplace: linking information security climate to compliant behavior, Journal of Information Privacy and Security 1 (3), 2005, pp. 18–41.

[8] W. Chin, Issues and opinion on structural equation modeling, MIS Quarterly 22 (1), 1998, pp. vii–xvi.

[9] J. Cohen, Statistical Power Analysis for the Behavioral Sciences, Lawrence Erlbaum Associates, Hillsdale, NJ, 1988.

[10] D.R. Compeau, C.A. Higgins, Computer self-efficacy: development of a measure and initial test, MIS Quarterly 19 (2), 1995, pp. 189–211.

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

[12] N. Friedkin, A Structural Theory of Social Influence, Cambridge University Press, Cambridge, 1998.

[13] K.H. Guo, Y. Yuan, N.P. Archer, C.E. Connelly, Understanding nonmalicious security violations in the workplace: a composite behavior model, Journal of Management Information Systems 28 (2), 2011, pp. 203–236.

[14] J.F. Hair Jr., R.E. Anderson, R.L. Thatham, W.C. Black, Multivariate Data Analysis, Prentice-Hall International, Inc., Upper Saddle River, NJ, 1998.

[15] S. Hazari, W. Hargrave, B. Clenney, An empirical investigation of factors influencing information security behavior, Journal of Information Privacy and Security 4 (4), 2009, pp. 3–20.

[16] T. Herath, H.R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organizations, European Journal of Information Systems 18 (2), 2009, pp. 106–125.

[17] T. Herath, H.R. Rao, Encouraging information security behaviors: role of penalties, pressures and perceived effectiveness, Decision Support Systems 47 (2), 2009, pp. 154–165.

[18] G.E. Higgins, B.D. Fell, A.L. Wilson, Digital piracy: assessing the contributions of an integrated self-control theory and social learning theory using structural equation modeling, Criminal Justice Studies: A Critical Journal of Crime, Law and Society 19 (1), 2006, pp. 3–22.

[19] T. Hirschi, Causes of Delinquency, Transaction Publishers, New Brunswick, NJ, 2002.

[20] Q. Hu, Z. Xu, T. Dinev, H. Ling, Does deterrence work in reducing information security policy abuse by employees? Communications of the ACM 54 (6), 2011, pp. 54–60.

[21] D. Iacobucci, G.A. Churchill, Marketing research: Methodological foundations (with Qualtrics Card), 10th ed., South-Western College Publishing, Cincinnati, OH, 2009.

[22] P. Ifinedo, An empirical study of ERP success evaluations by business and IT managers, Information Management & Computer Security 15 (4), 2007, pp. 270–282.

[23] P. Ifinedo, Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory, Computer & Security 31 (1), 2012, pp. 83–95.

[24] K.J. Knapp, T.E. Marshall, Information security: management's effect on culture and policy, Information Management & Computer Security 14 (1), 2006, pp. 24–36.

[25] A.G. Kotulic, J.G. Clark, Why there aren't more information security research studies, Information & Management 41 (5), 2004, pp. 597–607.

[26] S.M. Lee, S.-G. Lee, S. Yoo, An integrative model of computer abuse based on social control and general deterrence theories, Information & Management 41 (6), 2004, pp. 707–717.

[27] Y. Lee, K.A. Kozar, Investigating factors affecting the adoption of anti-spyware systems, Communications of the ACM 48 (8), 2005, pp. 72–77.

[28] Y. Lee, K.R. Larsen, Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software, European Journal of Information Systems 18 (2), 2009, pp. 177–187.

[29] L.N.K. Leonard, T.P. Cronan, J. Kreie, What influences IT ethical behavior intentions-planned behavior, reasoned action, perceived importance, or individual characteristics? Information & Management 42 (1), 2004, pp. 143–158.

[30] H. Li, J. Zhang, R. Sarathy, Understanding compliance with internet use policy from the perspective of rational choice theory, Decision Support Systems 48 (4), 2010, pp. 635–645.

[31] J.P. Meyer, N.J. Allen, A three-component conceptualization of organizational commitment: some methodological considerations, Human Resource Management Review 1 (3), 1991, pp. 61–98.

[32] B.-Y. Ng, A. Kankanhalli, Y.C. Xu, Studying users' computer security behavior: a health belief perspective, Decision Support Systems 46 (4), 2009, pp. 815–825.

[33] S. Pahnila, M. Siponen, A. Mahomood, Employees' behavior towards IS security policy compliance, in: Proceedings of the 40th Hawaii International Conference on System Sciences, January 3–6, Los Alamitos, CA, 2007.

[34] P.M. Podsakoff, S.B. MacKenzie, J.Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, Journal of Applied Psychology 88 (5), 2003, pp. 879–903.

[35] L.W. Porter, R.T. Mowday, R.M. Steers, The measurement of organizational commitment, Journal of Vocational Behavior 14, 1979, pp. 224–247.

[36] K. Rhodes, Operations security awareness: the mind has no firewall, Computer Security Journal 18 (3), 2001, pp. 27–36.

[37] R. Richardson, 2010 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2011 http://www.gocsi.com/survey.

[38] C.M. Ringle, S. Wende, A. Will, SmartPLS 2.0 (M3) beta, Hamburg (2005), http://www.smartpls.de.

[39] S.L. Robinson, A.M. O'Leary-Kelly, Monkey see, monkey do: the influence of work groups on the antisocial behavior of employees, Academy of Management Journal 41 (6), 1998, pp. 658–672.

[40] J. Rotter, Generalized expectancies for internal versus external control of reinforcement, Psychological Monographs 80 (1), 1966, pp. 1–28.

[41] J. Ryan, Information security tools and practices: what works? IEEE Transactions on Computers 53 (8), 2004, pp. 1060–1064.

[42] M.A. Sasse, S. Brostoff, D. Weirich, Transforming the weakest link – a human/computer interaction approach to usable and effective security, BT Technology Journal 19 (3), 2004, pp. 122–131.

[43] J.-Y. Son, Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies Information & Management 48 (7), 2011, pp. 296–302.

[44] A. Stajkovic, F. Luthans, Self-efficacy and work-related performance: a meta analysis, Psychological Bulletin 124 (2), 1998, pp. 240–261.

[45] J.M. Stanton, K.R. Stam, P.M. Mastrangelo, J.A. Jolton, Analysis of end user security behaviors, Computers & Security 24 (2), 2005, pp. 124–133.

[46] R.M. Steers, Antecedents and outcomes or organizational commitment, Administrative Science Quarterly 22, 1977, pp. 46–56.

[47] S. Taylor, P.A. Todd, Understanding information technology usage: a test of competing models, Information Systems Research 6 (2), 1995, pp. 144–176.

[48] M. Tenenhaus, V.E. Vinzi, Y.-M. Chatelin, C. Lauro, PLS path modeling, Computational Statistics & Data Analysis 48 (1), 2005, pp. 159–205.

[49] J.G. Thomas, R.W. Griffin, The power of social information in the workplace, Organizational Dynamics 18 (2), 1989, pp. 63–75.

[50] R. Thornton, Organizational involvement and commitment to organization and profession, Administrative Science Quarterly 15 (4), 1970, p. 417426.

[51] A. Vance, M. Siponen, S. Pahnila, Motivating IS security compliance: insights from habit and protection motivation theory, Information & Management 49 (3–4), 2012, pp. 190–198.

[52] C. Vroom, R. von Solms, Towards information security behavioural compliance, Computers and Security 23 (3), 2004, pp. 191–198.

[53] I.M.Y. Woon, A. Kankanhalli, Investigation of IS professionals' intention to practise secure development of applications, International Journal of Human-Computer Studies 65 (1), 2007, pp. 29–41.

[54] M. Workman, H.H. Bommer, D. Straub, Security lapses and the omission of information security measures: a threat control model and empirical test, Computers in Human Behavior 24, 2008, pp. 2799–2816.

Princely Ifinedo is an Associate Professor in the Shannon School of Business at Cape Breton University, Canada. He holds a doctoral degree in Information Systems Science from the University of Jyväskylä, Finland and master's degrees from the Royal Holloway University of London, UK and Tallinn University of Technology, Estonia. He has presented research at various international IS conferences, contributed chapters to several books/encyclopedias, and published in several reputable journals including JCIS, C&S, JSS, DATA BASE, CHB, JOCEC, JITM, IMDS, EIS, IJITDM, JITD, JITM, JGTIM, EG, JISP, and Internet Research. He has authored (and co-authored) over 90 peer-reviewed publications. He is affiliated with AIS, IEEE, ISACA, and CIPS.