Behaviour & Information Technology, Volume 43, Issue 3, 2024, pp. 523-539
DOI: 10.1080/0144929X.2023.2177825

Situational Support and Information Security Behavioural Intention: A comparative study using Conservation of Resources Theory

Yuxiang Hong*[a], Mengy Xu[b] & Steven Furnell[c]

a: Hangzhou Dianzi University, b: Cranfield University, c: University of Nottingham

Abstract

The formation of information security behavioural intention (ISBI) can be complex and dynamic in different contexts. This paper aims to examine and compare different users' ISBI formalization mechanisms when dealing with their personal affairs (non-work users) and organizational affairs (work users). Drawing on two principles of Conservation of Resources (COR) theory (i.e., resource loss principle, and resource gain principle), we developed two models to examine how situational support affects ISBI formation. The results of a study of 432 non-worker users and 261 work users indicate a curvilinear relationship between situational support and ISBI through subjective norms and risk perception for non-worker users, whilst a linear relationship via subjective norms is found for worker users. This is the first time that COR has been applied to explain the formation of ISBI. The findings broaden the research scope of individuals' ISBI by revealing how situational support affects the formalization mechanism for different users in cross-contexts. The theoretical and practical implications of the findings and the future study are discussed.

Keywords: Information security behavioural intention; situational support; risk perception; subjective norms; conservation of resources theory; social exchange theory

1. Introduction

The threat to information assets is a human and societal issue. It is widely acknowledged that information security behaviour plays a critical role in helping individuals or organizations decrease the probability of information security incidents (Furnell and Clarke, 2012; Snyman and Kruger, 2019). Moreover, the internal threat involving both malicious insiders and user negligence is one of the important causes of cyber-attack (IBM, 2021). Many studies have examined the formation of information security behaviour intention (e.g., Safa *et al*., 2016; Tsai *et al*.,2016; Thompson *et* al., 2017). They rationalised the information security behavioural intention (ISBI) formation process using classical theories of psychology, sociology, and criminology, such as the deterrence theory, theory of planned behaviour (TPB), and the protection motivation theory (PMT) (Moody *et al*., 2018). It is also found that other factors can affect the ISBI, such as security

Published by T&F. This is the Author Accepted Manuscript issued with: Creative Commons Attribution Non-Commercial License (CC:BY:NC 4.0).
The final published version (version of record) is available online at DOI:10.1080/0144929X.2023.2177825. Please refer to any applicable publisher terms of use.

education, training, and awareness (SETA) programs (Hu *et al*.,2021), employment status (Sharma & Warkentin, 2019); empowerment (Dhillon *et al*.,2020), imitation (Vedadi & Warkentin, 2020), emotions (Zhen *et al*., 2022). One consensus concluded from these studies is that the formation of ISBI is complicated and changeable (Li & Siponen, 2011). One of the key reasons is that individuals' information security behavioural decision-making can be impacted by the various contextual factors they surround, among which situational support (e.g. institutional guarantee, training, technical support) is argued to be critical to forming ISBI given it determines the availability of resources for the individuals (Warkentin *et al.*, 2011). However, little empirical research has examined ISBI formation by considering contextual factors with a focus on situational support. This study contributes further insights into this regard.

Specifically, this paper aims to examine how different users form their ISBI from the perspective of organizational behaviour. Li and Siponen (2011) identify the context affecting individuals' ISBI can be unpacked from two perspectives. One is 'place' (workplace/home), and the other is 'purpose' (work/non-work). In this study, we chose the perspective of 'purpose' to unpack the ISBI formation, therefore classifying non-work users and work users; the former deals with information security with personal affairs and the latter deals with it with organizational affairs. This definition has been widely used in previous studies (Anderson & Agarwal, 2010; Chen & Zahedi, 2016). Work users may gain high situational support such as information security training and advocacy of information security so that normalise their ISBI. Moreover, subjective norms, namely, individuals' perceived guidance from their peers, experts, or managers, can also signalise their information security behavioural decision-making (Warkentin et al., 2011). Comparably, the non-worker user lacks situational support from a specific stable supporter; their ISBI formation might be largely dependent on their self-risk perception and subjective norms with minimal specific situational support around. Risk perception is the paramount predictor in the ISBI process that determines the risk of property loss and privacy leakage (Vance et al., 2014). Therefore, we aim to investigate and compare differing performances in the ISBI formation process for non-work users, and work users. Researching ISBI formation in such a cross-context setting could contribute towards gaining a comprehensive understanding of the ISBI formation mechanism, and inform policy- and guidance-making for information security.

Given that ISBI formation refers to the person-environment interaction, this paper examines the ISBI from the perspective of organizational behaviour by drawing on the Conservation of Resources (COR) theory (Hobfoll, 2001, 2011; Hobfoll et al.,2018) and the Social Exchange Theory (SET) (Blau, 1964). The central tenet of COR is that people strive to obtain and maintain resources that help attain goals (Hobfall, 1989). In applying COR theory, we use resource depletion and investment processes to explain the links between situational support and ISBI. On the one hand, individuals tend to conserve their personal information assets to avoid loss. The increase of situational support will change the risk perception of personal information asset disclosure. On the other hand, with the situational support in information protection, individuals would feel obliged to develop the expected intention (i.e., more ISBI) and behaviours (i.e., ISB) towards the support giver drawn on SET. This can be an investment for gaining better recognition on their ISB from the support giver. The two theories are complementary and combine the capacity of resource at the individual level with resource exchange through situational support at the organizational level to explain the formation mechanism of ISBI. COR is often used to explain how individuals protect and gain their resources at the individual level; SET illustrates the reciprocity between the individual and the support giver, for example, the organization.

Drawing on the survey data of 432 non-work users and 261 work users, we adopted two theoretical models to examine how situational support affects their ISBI formation through subjective norms and risk perception. Our study makes three contributions. First, it improves the understanding of the ISBI formation mechanism from an organisational behavioural perspective and extends the scope of information security research by empirically comparing the two types of users' ISBI in cross-contexts. Second, we enrich the existing research that situational support impacts ISBI via mediators such as self-efficacy (e.g., Warkentin et al., 2011) by highlighting the direct effect of situational support on ISBI from the perspective of a reciprocity mechanism. Third, we indicate the role of situational support on ISBI via subjective norms from a resource investment perspective. Existing research such as Vedadi and Warkentin (2020) discussed a herd mentality as one type of avoidance behaviour from losses during ISBI. We found the positive angle of subjective norm, that is, individuals will evaluate whether to invest resources to meet the expectations of "important others". The findings have important practical implications for both organizations and individuals in both work and non-work contexts in enhancing their awareness of and effective responses to information security.

2. Conceptual and theoretical background

We first review the following key factors relevant to ISBI and theories to lay a conceptual foundation for theoretical and hypothesis development.

Situational Support

Situational support can be perceived as a social resource that helps obtain and maintain individual resources (Hobfoll, 2001). Warkentin *et al.* (2011) believe that individuals who are provided with situational support, such as guidance and resources from the organization or community, could improve their self-efficacy, resulting in improved performance. In the context of forming ISBI, situational constraint theory (Peters and O 'Connor, 1980) was used to indicate that situational constraints as an essential component impose constraints in the forming of ISBI (Warkentin *et al*.,2011). Conversely, emerging but limited research in information security found that providing resources to individuals, such as the available information security policies, passive support/active intervention, and the SETA program can stimulate the individuals' ISBI (Herath and Rao 2009; Han *et al*., 2017; Furnell *et al.*, 2018; Pérez-González *et al*., 2019).

Subjective Norms

Subjective norms are specific self-constrained behaviours from social pressure/expectations of family, friends, or other important referents. Studies have found that subjective norms positively affect an individual's information security attitudes (Cuganesan et al., 2018), their intention to use information protection technology (Dinev and Hu, 2007), and their information security policy compliance behavioural intention (Herath and Rao, 2009; Bulgurcu *et al*., 2010; Ifinedo, 2012). In the work domain, Fishbein and Ajzen (1975) argued that employees' subjective norms are affected by the expectations of supervisors and colleagues. The social pressures from these sources could affect the decision-making process of behaviour, such as perceived behavioural control (self-efficacy) and attitude toward information security (Guo *et al*., 2011; Warkentin *et al*., 2011; Hong and Furnell, 2019).

Risk perception

Risk perception is widely recognised as a predictor of security behaviours when evaluating the loss severity and probability of adverse events (Renn and Swaton, 1984; Renn, 1998). Hong *et al*. (2019) found that risk perception has a positive impact on individuals' emergency preparedness behaviours. van Schaik *et al*. (2017) regarded risk perception as an important predictor of information security behaviour in terms of

cognitive and affective dimensions (Loewenstein *et al*., 2001; Peters *et al*., 2004; Weber, 2006; Sundblad *et al*., 2007; Janssen *et al*., 2012; Trumbo *et al*., 2016). The cognitive dimension refers to an increase in the knowledge of threats (Sundblad *et al*., 2007), which can be constructed and developed from independent learning, such as education and on-the-job training. The affective dimension refers to an emotional feeling towards external stimuli (Slovic *et al*., 2007). Both risk dimensions have been identified as predictors of behavioural intentions (Loewenstein *et al*., 2001).

Conservation of Resources (COR) theory

COR explains the motivation of individuals' behaviour from the perspective of resources. It suggests that organizations can offer situational resources for employees to alleviate the strain and facilitate positive attitude and performances (Hobfoll, 2001). The resources are '*those objects, personal characteristics, conditions, or energies that are valued by the individual or that serve as a means for the attainment of these objects, personal characteristics, conditions, or energies* (Hobfoll, 1989, p. 516)'. Resource loss and gain can be used to predict actions (Hobfoll, 1989). Behaviour prediction follows two principles: The resource loss principle of COR is concerned with the negative impact of losing key resources due to stress and strain on individual motivation and behaviours, while the resource investment principle of COR depicts people's motivations to protect their current resources and acquire new resources. Although information security behaviours are usually explained as behaviours of protecting the organization or individual's "resource" (Ifinedo, 2018), a theoretical framework from a resource perspective is largely under-documented in empirical research on information security.

Social Exchange Theory (SET)

SET is widely used to explain the economic and psychological exchange behaviour between two parties (Blau, 1964). This indicates that individuals who perceive social support tend to develop reciprocating behaviours towards the support giver. There are different types of social support that a person can receive, namely affective, instrumental, and informational (Settoon *et. al*., 1996). In the context of information security, affective support can be the security care delivered by the other party. Instrumental support includes the security training and policy protection offered to individuals from other parties. Informational support refers to the delivery of security information that is helpful to individuals' information security. It is evident from a few information security studies that employees who received positive safety and security support from organizations (i.e.

security training, security inspections, and high status of security managers) are more willing to appreciate the organizational commitment to safety and security (Hofmann and Morgeson, 1999; Mearns and Reader, 2008; DeJoy et al., 2010). Therefore, they tend to reciprocate such social support with more secure and safe behaviours as organizations expected (Huang et al., 2016).

3. Theoretical framework

In seeking to understand different users' ISBI formation processes, we drew upon COR and SET to analyse how situational support as a resource drives individuals' intentions to engage with information security behaviours through subjective norms and risk perceptions. We propose two models (model 1 and model 2) that depict the relationship of situational support and ISBI, and justify how these models fit for the non-work user and work user respectively.

We argue the principle of resource loss is more suited for non-work users because they can only gain unstable and limited situational support compared to the work user. In a situation that lacks support, non-work users tend to protect or recover resources from the loss. Comparably, work users tend to be offered stable and designated social support from their organisation (e.g., Pluut et al., 2018), According to the COR theory's corollary, "*individuals with resources are better positioned for resource gain*" (Halbesleben et al., 2014, p. 1338) that benefits themselves and organizations via the reciprocity mechanism. Therefore, the "resource gain principle" and SET are more suited for work users.

SS and ISBI via risk perceptions and subjective norms: Through the lens of COR's 'resource loss'

We argue the relationship between situational support and ISBI is not linear but curvilinear and dynamic, where individuals' risk perceptions and subjective norms each play roles. The principle of resource loss states that resource loss rather than gains has greater impact on individual behaviour (Hobfoll, 2001). This is because an individual's risk perception of resource loss tends to be more sensitive, therefore in information security literature, information resource loss is found to be the key factor in forming ISBI (Vance *et al.*, 2014). When receiving situational support, individuals' risk perception can change from affective and cognitive dimensions thus making different impacts in forming ISBI. A low level of situational support related to information security may not be sufficient for individuals to acquire information and knowledge to enhance cognitive risk perceptions (Sundblad *et al*., 2007). One of the main reasons is that individuals who do

not know or experience a cyber disaster might overestimate the risks (Hong *et al*., 2019). Meanwhile, individuals may perceive high affective risk as they worry about the possibility of resource loss when confronted with the unknown. Individuals' fear and anxiety can be amplified when the people around them view information security as a risk and take related precautions.

While individuals reduce their concerns about resource depletion with increasing situational support (Hobfoll, 2011), the affective and cognitive dimensions of their risk perceptions are not dropped at the same pace. The affective risk perception could directly decrease, but it takes longer to reduce cognitive risk perception (Mitchell, 2005; Lauver *et al*., 2009). This is because people's cognitive evaluations apprehended from training, education, persuasion, etc respond slower than their affective reactions (Zajonc, 1980; Loewenstein *et al*.,2001). Therefore, cognitive risk perception may remain at a relatively higher level for a period of time even though affective risk perception has dropped significantly. Moreover, individuals gradually enhance their cognitive risk perception with the situational support increasing. In a resourceful environment that offers security information and training, the enhanced cognitive risk perceptions could motivate individuals to develop relevant security understanding and skills such as using anti-virus, firewall configuration, phishing site identification, etc. (Mitnick, 2002; Puhakainen and Siponen, 2010), all of which facilitate individuals to form their ISBI (Herath and Rao, 2009; Warkentin *et al*., 2011).

Based on the discussions above, we proposed the following hypotheses:

- ***H1***: Situational support and ISBI have a U-shaped curvilinear relationship according to the principle of resource loss.
- ***H2***: Situational support and risk perception have a U-shaped curvilinear relationship according to the principle of resource loss.
- ***H3***: Risk perception has a significant mediating effect on the U-shaped curvilinear relationship between situational support and ISBI according to the principle of resource loss.

The relationship between situational support and risk perception is argued to be moderated by the subjective norm. Situational support, especially from the organization, is embedded with expectations on certain behaviours, which could either motivate or

pressurise employees to form both affective and cognitive risk perceptions. For an individual who has a high level of subjective norms to information security, since their self-contained behaviours are highly dependent on other informant's expectations and requirements, their risk perceptions of information security are more likely to be boosted with the increasing situational support, compared to those with a lower level of subjective norms (Kasperson et al.,1988; van der Linden, 2015). That is, individual subjective norms might alleviate the relationship between the situational support they received and their risk perceptions. Hypothesis 4 is thus proposed:

- ***H4***: Subjective norms have a significant moderating effect on the U-shaped curvilinear relationship between situational support and risk perception according to the principle of resource loss.

The theoretical framework based on COR's 'resource loss' principle is shown in Figure 1.

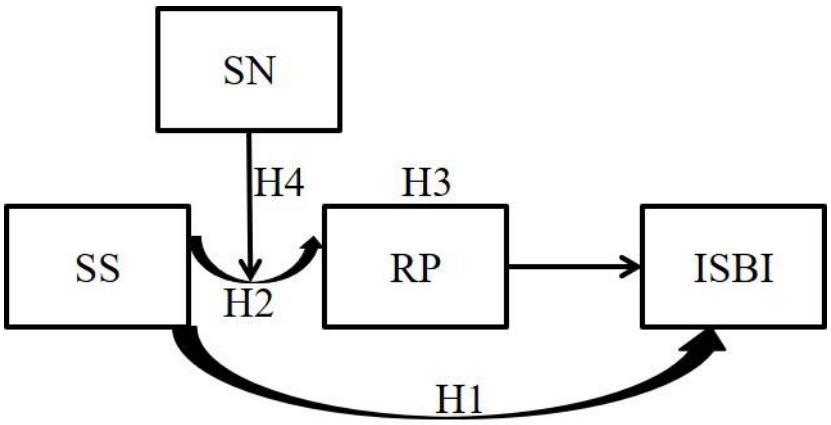

Figure 1. Model 1. A Theoretical framework based on COR's 'resource loss'

SS and ISBI via subjective norms: Through SET and the Lens of COR's 'resource investment'

According to SET, individuals who perceive situational support from the organization in terms of security tend to generate ISBI. Individuals are more likely to engage in information security-related affairs when they are trained and supported by related resources. This is verified in Hofmann and Morgeson (1999), showing that the more situational support individuals perceive, the more likely they are to be motivated to perform the expected behaviours from the support giver (in this case, the higher possibility they will perform safety behaviours). Moreover, according to the principle of resource investment, people obtain and invest resources to protect against resource loss,

recover from losses, and gain extra resources (Hobfoll, 2001). In the context of information security, it is arguable that the more situational support the individual perceives in relation to security, the more likely they are to protect personal and organisational assets from loss. Hypothesis 5 is thus proposed:

- ***H5:*** Situational support has a linear positive effect on ISBI according to the principle of resource investment.

Individuals' subjective norms can affect the occurrence and extent of social exchange. Subjective norms can be shaped by social interactions with exchange partners (e.g. organization, colleagues in the workplace etc.). We argue that a stronger ISBI may emerge when exchange partners attach importance to information security measures. This is because, people perceive social pressures to meet organizational and peer expectations (Herath and Rao, 2009; Li *et al*., 2010; Ifinedo, 2012); with the subjective norms shaping, the individual may persist in the belief that implementing security measures is an essential and useful way to engage with the organization (Guo *et al*., 2011). However, if exchange partners take an indifferent attitude towards security measures, and norms are unlikely to be fostered, people may undervalue information security and perform less ISBI (Yukl, 2002). Individuals may have limited personal resources, such as time, physical energy, and attention (Ng and Feldman, 2012), and if they are unaware of the importance of information security and/or tend to allocate their resources to other areas, their intentions to perform informal security behaviours might not high. Therefore, hypothesis 6 is proposed:

- ***H6:*** Subjective norms have a significant moderating effect on the relationship between situational support and ISBI according to the principle of resource investment.

The theoretical framework based on COR's 'resource investment' principle is shown in Figure 2.

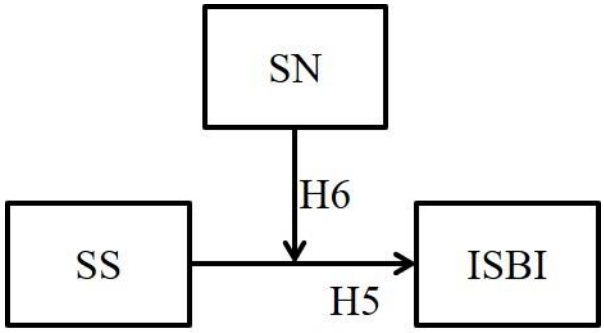

Figure 2. Model 2.A Theoretical framework based on the 'resource investment' of COR

SS and ISBI between non-work users and work users

The ISBI formation mechanism can be heterogeneous for non-work users and work users given the situational support of information security around them varies. We suggest that the relationship between situational support and ISBI for non-work users tends to conform to Model 1, while work users are more likely to conform to Model 2.

Non-work users could benefit from receiving situational support for information security to mitigate and prevent unnecessary risks in their daily life. Situational support varies from day to day considerably (Halbesleben et al., 2014). Compared to work users, non-work users have fewer channels to receive specific situational support, and their personal risk perception can play a significant role in forming their ISBI. If an individual has a higher level of risk perception of resource loss (e.g., personal information and privacy), they tend to form ISBI (Guo et al., 2011; Hong and Thong, 2013; Vance et al., 2014).

.

Subjective norms as specific self-constrained behaviours could moderate non-work users to form the ISBI. In contrast to work users, while non-work users are less likely to be affected by peer pressures and expectations from supervisors and colleagues; with a high level of subjective norms, an individual's risk perceptions can be boosted with the increasing situational support, compared to those who have a lower level of subjective norms and verse vice (Kasperson et al.,1988; van der Linden, 2015).

For work users, the loss of organizational information assets may not directly affect their privacy or property safety because organizational information security may lack personal relevance, thus rendering the consideration of risk perception unnecessary (Johnston *et al*., 2015; Menard *et al*., 2017). The intention of work users on information security behaviour, however, tends to be associated with their intentions of organizational

compliance or organizational citizenship behaviour that often link to work users' job performance. Therefore, with situational support from the organisation, employees can be motivated to demonstrate security behaviours to comply and engage with the organizational policy and guidance.

4. Method

For this research, we used a scenario-based survey to examine the ISBI formation mechanism among non-work users and work users, and to empirically test the proposed models. Participants were asked to read scenarios regarding information security before answering associated questions. Example questions include if they were the character/role in the particular scenario, what would they do? The reason for using the hypothetical scenario research design is that questionnaires tend to be sensitive and demotivate the respondents' willingness to answer, thereby impacting the survey response rate (Kotulic and Clark, 2004). The scenario has an unthreatening manner of dealing with sensitive issues (Nagin and Pogarsky, 2001). In addition, when participants characterise their behavioural intentions from a third-person perspective, the social expectations biases can be significantly reduced, which can enhance the research quality (Wason *et al*., 2002). This method has been effectively applied and validated in other studies of ISBI (Guo *et al*., 2011; D'Arcy *et al*., 2009; Vance *et al*., 2012).

The studies mentioned above have looked at the work users scenarios, in order to improve the reliability of the measurement and structural validity of the research, the scenario design for work users was first based on empirically validated scenarios from existing research, and then cautiously contextualised by considering a series of realistic and practical factors related to information security. For non-work users, the scenarios were self-developed based on an open-ended questionnaire survey and content analysis of one hundred college students. Prior to the survey, the scenario was piloted with twenty eligible participants (ten non-work users and ten work users) to help probe the suitability of the hypothetical scenarios and questions. The findings of the pilot study indicated that the scenario design was clear and appropriate for this research. The specifications of the scenario have been published in two papers by the Authors (2019, 2021).

4.1 Participants and data collection

As part of a larger study on ISBI (Authors, 2019, 2021), the data was collected using web- and paper-based surveys for non-work users and work users, respectively. Each

questionnaire was accompanied by a cover letter, an information sheet, and a consent form. Full-time university students represented the non-work user group (Anderson and Agarwal, 2010; Dang-Pham and Pittayachawan, 2015; Liang and Xue, 2010; Tu *et al*., 2015), who usually receive situational support from universities (Kim, 2013, 2014). A total of 500 web-based questionnaires were distributed to university students in Zhejiang Province, China through the survey platform WenjuanWang (www.wenjuan.com) via the random sampling method. A total of 432 valid non-work users' questionnaires were collected amounting to 86.4% of the total response rate, of which 49.3% were male respondents and 50.7% were female respondents.

For work-users, 500 paper-based questionnaires were sent to 100 companies in the IT, finance, manufacturing, logistics, real estate, hotels and restaurants, and media entities in Zhejiang Province, China. Each firm received a certain number of questionnaires based on the size of the company and their willingness to participate, with an average of five copies provided to each firm. The gender, rank, and profession of the participants were considered while distributing the questionnaires. A total of 261 valid work users' questionnaires were collected, with a 52.2% response rate; 56% were male respondents and 44% were female respondents.

4.2 Measures

The measures employed in this study originate from mature classical scales with a 5-point Likert-type scale ranging from *strongly disagree* to *strongly agree*. The questions investigating ISBI and subjective norms were modified from the questionnaires developed by Ifinedo (2012), and the questions investigating situational support were modified from the questionnaires developed by Warkentin *et al*. (2011). As risk is usually considered to be the product of severity and probability (Chang *et al.*, 2015; Ni *et al.*, 2007; Wolff *et al*., 2019), risk perception was measured by computing the geometric average of two independent items, perceived severity and perceived vulnerability derived from Ifinedo (2012) and Workman *et al*. (2008), respectively. In addition, this study also chose gender (Hearth and Rao, 2009; Li *et al*., 2010; Vance *et al*., 2012) and scenario (Guo *et al*., 2011; D'Arcy *et al*., 2009; Vance *et al*., 2012) as control variables. The final set of measure items used for this study is presented in the appendix.

4.3 Data analysis

This study examined the suitability of different groups (work and non-work users) to two hypothetical models based on two principles of COR theory. SPSS 19.0 and R 4.0.2 (packages of "ggplot2" and "interactions") were used to analyse the data. The data analysis procedure consists of three steps, as shown in Figure 3.

Step 1: Preliminary analysis. Cronbach's alpha coefficient was used to measure the internal consistency of the measurement results. The general rule is that a Cronbach's alpha > 0.70 indicates good reliability. Confirmatory factor analysis (CFA) was used to test convergent and discriminant validity. The general rule is that if all the loadings of the items are higher than 0.50, all the values of composite reliability (CR) are higher than 0.7, and all values of average variance extracted (AVE) are higher than 0.5, the convergent validity is good. Moreover, if the square root of AVE for each construct is higher than the correlations between it and all other constructs, the discriminant validity is good (Fornell & Larker, 1981).

Step 2: Main effect testing. A hierarchical regression analysis was used to test the hypotheses of the direct relationships, especially the effects that situational support impact on ISBI in two models based on the 'resource loss' and 'resource investment' principles as well as the effect that situational support impact on risk perception in the model based on the 'resource loss' principle.

Step 3: Mechanism analysis. We used MEDCURVE provided by Hayes (Hayes, 2013) and estimated 5,000 bootstrap samples to test the mediating effect of nonlinear relationships. Following the procedure suggested by Aiken & West (1991) we tested the moderating effect, and use Johnson-Neyman technique via PROCESS (model 1, also provided by Hayes) to test the conditional effect of the predictor variable on the dependent variable at various values of the moderating variable.

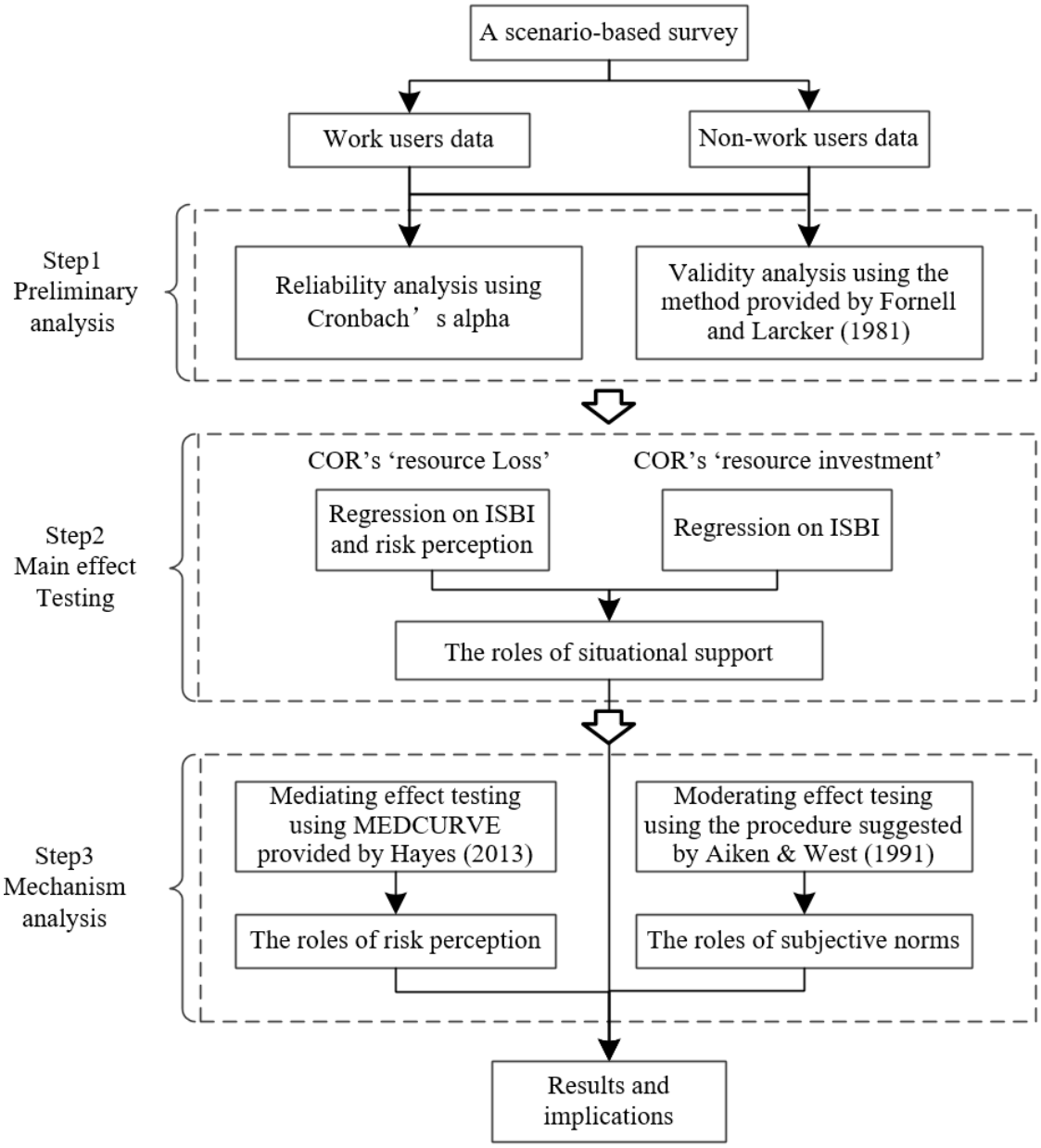

Figure 3. Data analysis procedure.

5.Results

5.1 Preliminary analysis

We first conducted an internal consistency reliability analysis to examine the qualities of the given scales and acquired samples. The results indicated a high internal consistency for the three scales (Cronbach's alpha = 0.84 for ISBI, 0.89 for situational support, and 0.86 for subjective norms). We did not calculate the Cronbach's alpha of risk perception because it is the geometric average of two independent single items, namely perceived severity and perceived vulnerability.

We then conducted a CFA for situational support, subjective norms, and ISBI based on the total samples. The results indicated that the Kaiser-Meyer-Olkin value was 0.827 > 0.7, and Bartlett's test of sphericity was significant, indicating that the sample size was adequate, and the data could be subjected to factor analysis. As illustrated in Table 1, all loadings of these items were higher than 0.50, all the values of composite reliability (CR) were higher than 0.7, and all values of average variance extracted (AVE) were higher than 0.5. Therefore, convergent validity was good. As shown in Table 2, the square root of AVE for each construct is higher than the correlations between it and all other constructs, indicating good discriminant validity (Fornell and Larcker, 1981).

In addition, Means, standard deviations, and correlation coefficients among the variables are reported in Table 2. Almost all variables were significantly correlated for both groups, except risk perception and ISBI for the work users' group. All the correlation coefficients were lower than 0.7, preliminarily indicating that the multicollinearity problem was not severe. This was further verified by the indicator of variance inflation factor (VIF). The results (in Table 2) showed that all the VIFs were lower than 1.5, well below the threshold of 10 (Asteriou & Hall, 2011).

Table 1 Factor Loading of Items

Construct	Item	Loading	CR	AVE
ISBI	ISBI1	0.872	0.867	0.765
	ISBI2	0.877		
SS	SS1	0.876	0.910	0.771
	SS2	0.913		
	SS3	0.843		
SN	SN1	0.780	0.856	0.664
	SN2	0.837		
	SN3	0.827		

Note: ISBI=information security behavioural intentions; SS=situational support; SN=subjective norms.

Table 2 Mean, SD, and Correlations for four factors, ISBI, SS, SN, RP

Variables	Groups	Mean	SD	ISBI	SS	RP	SN	VIF
ISBI	Total	4.02	0.87	0.87†				
	non-work users	3.96	0.93					
	work users	4.11	0.76					
SS	Total	3.38	0.98	0.31**	0.88†			1.328

	non-work users	3.13	1.02	0.31**				1.281
	work users	3.78	0.74	0.27**				1.475
RP	Total	3.43	0.94	0.22**	0.23**	-		1.183
	non-work users	3.52	0.97	0.34**	0.35**			1.279
	work users	3.28	0.87	0.01	0.14**			1.034
SN	Total	3.93	0.83	0.58**	0.49**	0.33**	0.81†	1.449
	non-work users	3.82	0.89	0.65**	0.43**	0.43**		1.378
	work users	4.12	0.67	0.40**	0.57**	0.18**		1.494

Note: ** $p < 0.01$, * $p < 0.05$,† are square roots of AVE; total sample number = 693, sample number of non-work users = 432, and sample number of work users =261; RP = risk perception; VIF = variance inflation factor.

5.2 Hypothesis Testing

5.2.1 Main Effect Testing

A hierarchical regression analysis was used to test the hypotheses in this study. As indicated in Table 3, ISBI was considered as the dependent variable for the non-work user group. The results revealed that situational support had a significant U-shaped curvilinear effect on ISBI (Model 3, $\beta=0.17$, $p < 0.001$). *Hypothesis 1* was thus supported for non-work users. Next, we performed the same analysis for the work user group. The results as revealed in Table 4, indicate that the curvilinear relationship between situational support and ISBI is not significant (Model 9, $\beta=0.12$, $p = 0.069$); however, situational support had a significant positive linear effect on ISBI (Model 8, $\beta=0.28$, $p < 0.001$). *Hypothesis 1* was thus not supported for work users, whereas *Hypothesis 5* was. Figure 4 illustrates the difference in the relationship between situational support and ISBI for both non-work users and work users.

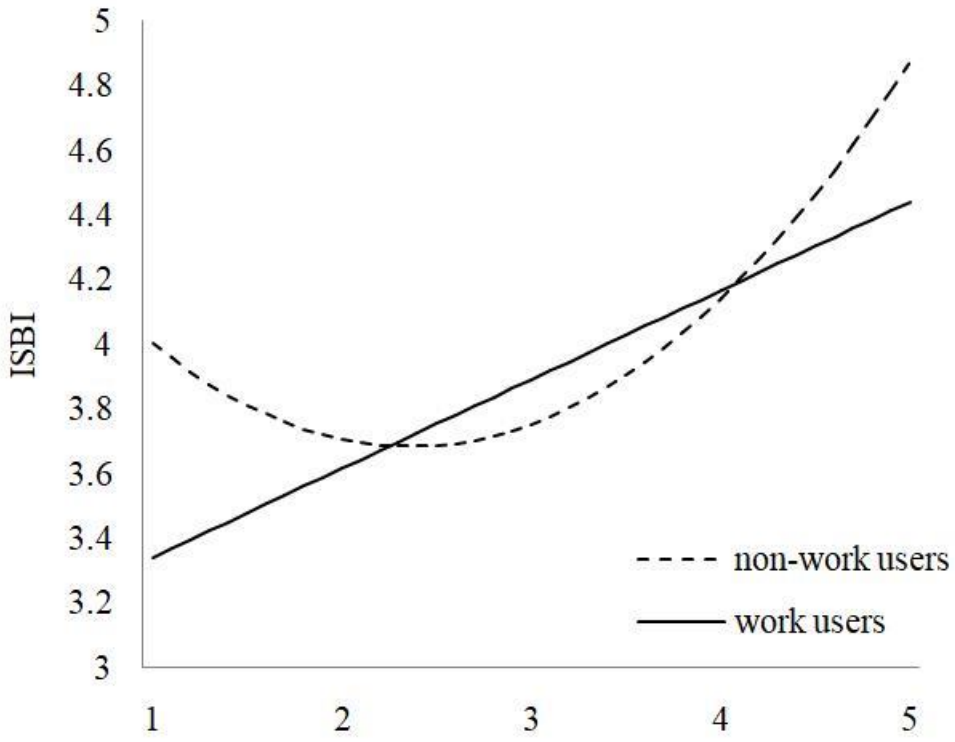

Figure 4. Relationship between situational support and ISBI

As presented in Table 5, the risk perception was considered as the dependent variable. The results indicated that situational support had a significant U-shaped curvilinear effect on risk perception (Model 14, β=0.14, $p < 0.001$). *Hypothesis 2* was thus supported for non-work users. As presented in Table 6, when the same analysis was conducted in the work users' group, the results revealed that the curvilinear relationship between situational support and risk perception was not significant (Model 19, β=0.02, $p = 0.812$); however, situational support had a significant positive linear effect on risk perception (Model 18, β=0.156, $p < 0.05$).

Table 3 Regression results on ISBI of non-work users

	M1		*M2*		*M3*		*M4*		*M5*		*M6*	
	β	*p*	*β*	*p*	*β*	*p*	*β*	*p*	*β*	*p*	*β*	*p*
Gender	-0.17	0.052	-0.09	0.308	-0.06	0.448	-0.08	0.312	-0.07	0.297	-0.07	0.335
Scenario	-0.05	0.096	-0.06	0.062	-0.05	0.123	-0.03	0.251	-0.02	0.406	-0.02	0.386
SS			0.28**	<0.001	-0.78**	<0.001	-0.67**	0.001	-0.50	0.003	-1.36	0.056
SS^2					0.17**	<0.001	0.14**	<0.001	0.08	0.002	0.28	0.023
RP							0.20**	<0.001				
SN									0.63	<0.001	0.50	0.047

SS×SN									0.18	0.309
SS^2×SN									-0.04	0.150
R^2	0.014		0.103		0.158		0.195		0.444	

Table 4 Regression results on ISBI of work users

	M7		*M8*		*M9*		*M10*		*M11*	
	β	*p*	*β*	*p*	*β*	*p*	*β*	*p*	*β*	*p*
Gender	0.15	0.114	0.16	0.045	0.17	0.070	0.13	0.151	0.08	0.357
Scenario	-0.03	0.303	-0.02*	0.446	-0.03	0.414	-0.02	0.597	-0.02	0.477
SS			0.28**	<0.001	-0.59	0.224	0.08	0.298	-1.07**	0.005
SS^2					0.12	0.069				
SN							0.399**	<0.001	-0.60	0.071
SS×SN									0.27**	0.002
R^2	0.01		0.09		0.10		0.17		0.20	

Table 5 Regression results on RP of non-work users

	M12		*M13*		*M14*		*M15*		*M16*	
	β	*p*	*β*	*p*	*β*	*p*	*β*	*p*	*β*	*p*
Gender	-0.03	0.738	0.08	0.397	0.10	0.271	0.09	0.271	0.10	0.247
Scenario	-0.07*	0.050	-0.07*	0.025	-0.06*	0.049	-0.05	0.110	-0.05	0.069
SS			0.34**	<0.001	-0.56**	0.008	-0.41*	0.044	1.57	0.070
SS^2					0.14**	<0.001	0.10**	0.002	-0.23	0.121
SN							0.33**	<0.001	1.00**	0.001
SS×SN									-0.50*	0.019
SS^2×SN									0.08*	0.020
R^2	0.01		0.14		0.17		0.24		0.25	

Table 6 Regression results on RP of work users

	M17		*M18*		*M19*		*M20*		*M21*	
	β	*p*	*β*	*p*	*β*	*p*	*β*	*p*	*β*	*p*
Gender	-0.10	0.372	-0.08	0.472	-0.08	0.460	-0.11	0.324	-0.12	0.291
Scenario	<0.001	0.997	0.05	0.884	0.01	0.889	0.01	0.797	0.01	0.820
SS			0.156*	0.034	0.02	0.970	0.05	0.568	-0.18	0.690

SS^2				0.02	0.812				
SN						0.20	0.039	-0.01	0.991
SS×SN								0.06	0.605
R^2	0.003		0.020	0.037		0.037		0.038	

5.2.2 Mediating Effect Testing

We entered risk perception based on Model 3 to verify the mediating effect of risk perception on the U-shaped curvilinear relationship between situational support and ISBI for the non-work user group. The results indicated that the effect of risk perception was significant (Model 4, $\beta = 0.20$, $p < 0.001$), although the effect of situational support (Model 4, $\beta = -0.67$, $p < 0.01$) and the square of situational support (Model 4, $\beta = 0.14$, $p < 0.001$) had decreased. We then used MEDCURVE (Hayes, 2013) and estimated 5,000 bootstrap samples in which the independent variable was situational support, the mediator was risk perception, and the dependent variable was ISBI. The results revealed that when situational support was at a moderate level (mean value; 95% CI = [0.0335,0.1146]) and at a high level (mean value plus one standard deviation; 95% CI = [0.1256,0.2256]), the confidence estimation of the indirect effect of situational support affecting ISBI through risk perception did not include 0, whereas, when situational support was at a low level (mean value minus one standard deviation; 95% CI = [-0.0328,0.0572]), the confidence estimation of the indirect effect of situational support affecting ISBI through risk perception included 0. This result indicated that the curvilinear relationship between situational support and ISBI revealed a significant partial mediation by risk perception when situational support was at a moderate and high level. Therefore, *Hypothesis 3* was partly supported for non-work users. Meanwhile, as the correlation coefficient between risk perception and ISBI was not significant, it indicated that risk perception does not have a mediating effect on the relationship between situational support and ISBI for work users. Thus, *Hypothesis 3* was not fully supported for work users.

5.2.3 Moderating Effect Testing

Table 5 presents the result of the moderating effect of subjective norms on the relationship between situational support and risk perception for the non-work user group, where risk perception was considered as the dependent variable. We entered subjective norms in Model 15, and then entered the interaction items of subjective norms and situational support (SN × SS) as well as the interaction items of subjective norms and square of

situational support (SN × SS^2) in Model 16. The results indicated that the effects of both SN × SS (Model 16, β = -0.50, p < 0.05) and SN × SS^2 (Model 16, β = 0.08, p < 0.05) were significant. *Thus, Hypothesis 4* was supported for non-work users. The interaction effects of situational support and risk perception are illustrated in Figure 5. We also tested the moderating effect of subjective norms' impact on the relationship between situational support and risk perception for the work user group. The results revealed that the effect of SN × SS (Table 6, Model 21, β = 0.06, p = 0.605) was not significant.

Table 3 presents the result of the moderating effect of subjective norms on the relationship between situational support and ISBI for the non-work user group, where ISBI was considered as the dependent variable. The results revealed that the effects of both SN × SS (Model 6, β = 0.18, p = 0.309) and SN × SS^2 (Model 6, β = -0.04, p = 0.150) were not significant. For the work user group, as presented in Table 4, SN×SS had a significant effect on ISBI (Model 11, β = 0.27, p < 0.01). The interaction effects between the SS and ISBI are presented in Figure 6.

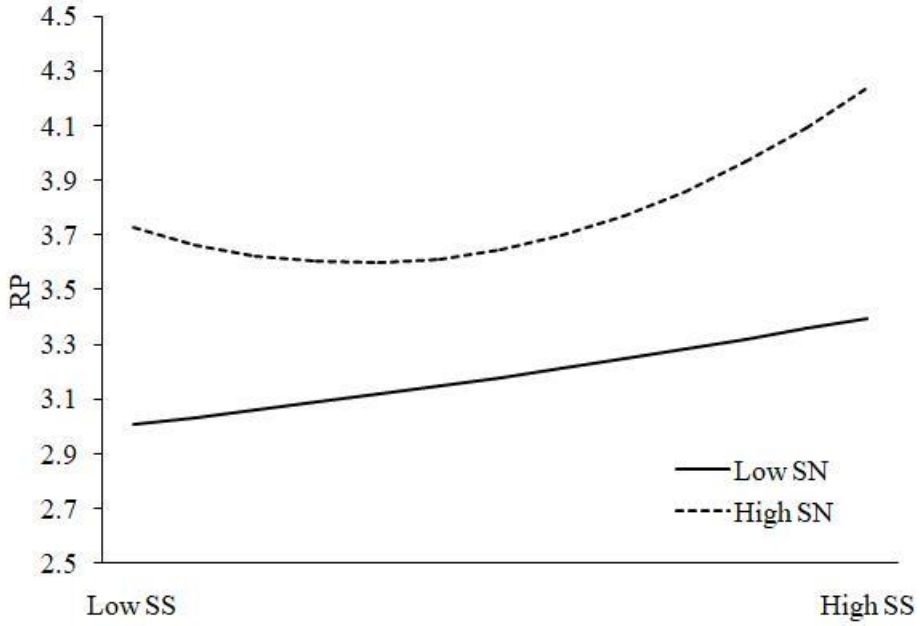

Figure 5. Moderating effect of SN on the relationship between SS and RP in the non-work user group

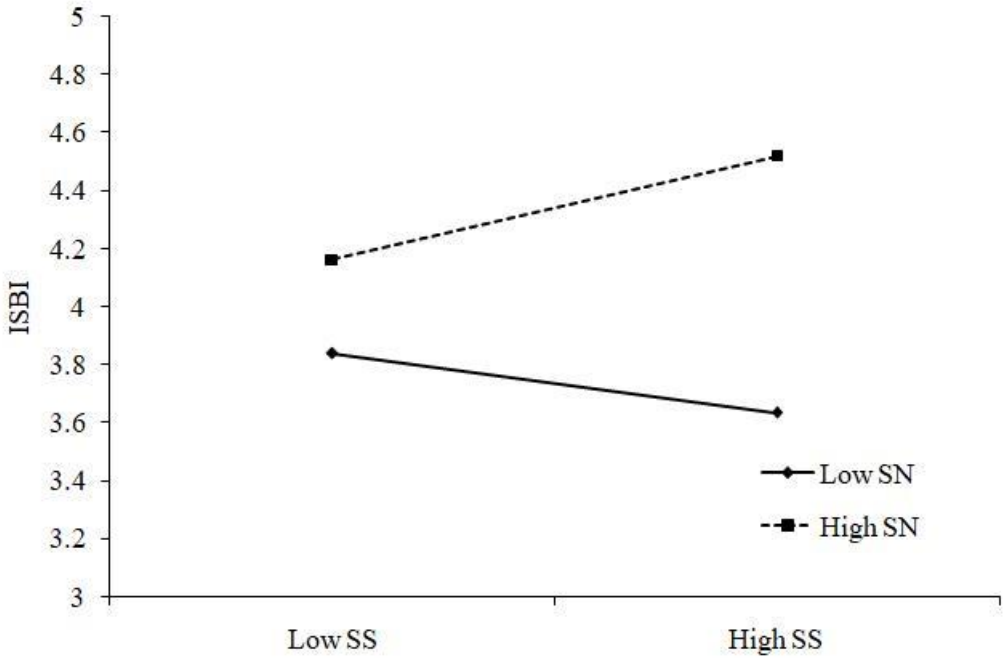

Figure 6. Moderating effect of SN on the relationship between SS and ISBI in the work user group

To further examine the moderating effect of subjective norms on the relationship between situational support and ISBI, we used PROCESS (Model 1) provided by Hayes (2013) using 5,000 bootstrap samples and analysed the conditional effect of situational support on ISBI at degrees of the subjective norms based on the Johnson-Neyman technique. As demonstrated in Figure 7, when subjective norms are lower than 3.01, situational support has a negative effect on ISBI, whereas when subjective norms are higher than 4.44, the effect of situational support on ISBI is significantly positive. Therefore, *Hypothesis 6* was supported for work users.

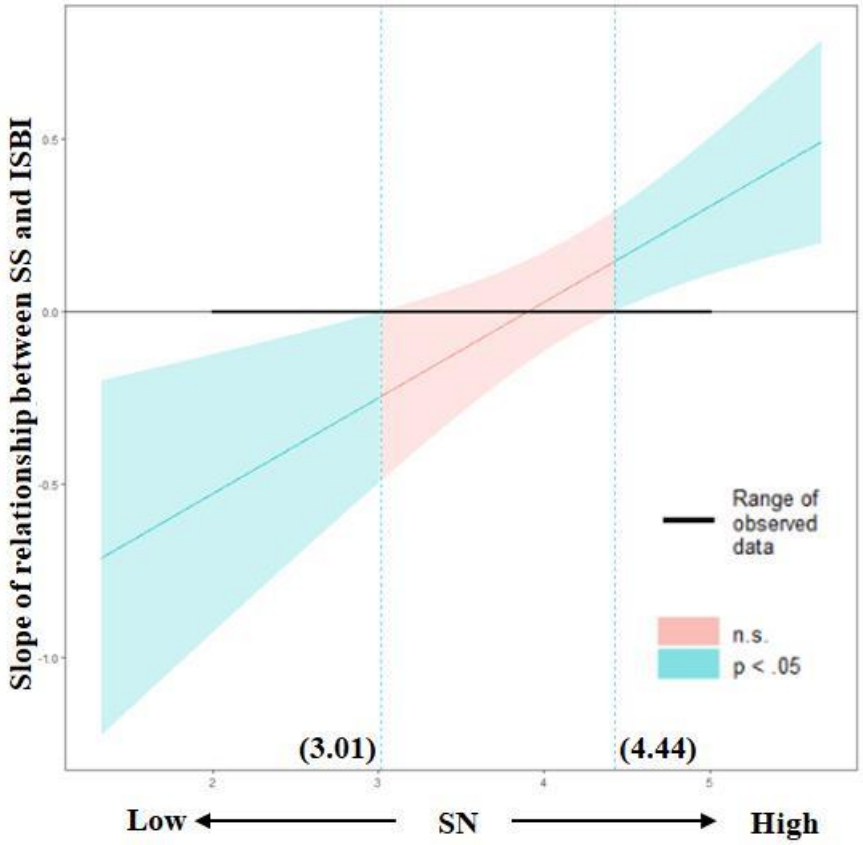

Figure 7. Condition effect of SS on ISBI in the work user group. The polygon shaded in blue indicates a 95% CI using the Johnson-Newman technique.

6. Discussion

This study examined and compared the ISBI formalization mechanism for non-work and work users in the context of situational support. We found that support had a significant positive effect on ISBI for work users. This is consistent with the study of Warkentin et al. (2011), where verified the positive effect of situational support on the intention to protect patient privacy among employees of healthcare organizations. However, Warkentin et al. mainly considered the mediating effect of self-efficacy on the relationship between situational support and ISBI but did not attribute the direct effect from the perspective of the reciprocity mechanism. The findings of the current study imply that work users who perceive situational support in information security provided by the organization would have a high intention to engage with information security performance.

Moreover, we also considered the boundary of this relationship. Our findings show that the prerequisite of this positive effect is that the subjective norms of work users are at a

high level. This echoes Vedadi and Warkentin (2020)'s study, where they discussed a herd mentality during the decision-making of information security behaviour, and clearly illustrated the difference between herd behaviour and subjective norms from the perspective of information sources as well as how information is acquired. In addition to this, we unpacked that one more difference between these two concepts that is, herd behaviour is one type of avoidance behaviour from losses related to a bad choice, while subjective norm is related to investment decision-making through being consistent with the behaviours of "important others". That is, situational support can positively impact ISBI only if people perceive information security measures as compulsory for organizations based on the judgment of expectations from "important others". When subjective norms are at a very low level, increased situational support does not make an impact in forming ISBI. This is because when employees do not regard the implementation of information security measures as necessary and beneficial, employees will reciprocate the situational support provided by the organization with other actions beneficial to job performance. This is drawn on SET that individuals would reciprocate the support giver by maximizing their efforts (Settoon *et al.*, 1996). This resource re-investment or reallocation will lead to resource gains in the future (e.g., continuing situational support) based on the logic of resource investment principle (Hobfoll, 2018).

The formation mechanism of ISBI for non-work users shows a U-shaped curvilinear relationship between situational support and ISBI. Regardless of whether the situational support is at a low or high level, our study found that non-work users show a higher level of ISBI. This is because when the situational support is none or limited, the psychological insecurity caused by lacking resources might drive non-workers to form ISBI. This finding is consistent with the previous study that discusses the positive impact of fear appeals on ISBI based on PMT where fear is seen as a negative emotion to danger (Boss et al., 2015). Until the situational support is sufficiently high, non-work users are provided with more established awareness of information security. Adequate situational support, including training and other mechanisms, facilitate policy compliance, meaning that available resources can lead to a positive impact on ISBI (Herath & Rao, 2009). However, when the situational support is at a medium level, non-workers might not yet form a solid ISBI as the awareness and capacity of cognitive formation of information security remain under the process. This is consistent with what Warkentin *et al.* (2011) found in their research; that there is a mediating effect of self-efficacy on the relationship between situational support and ISBI.

Individuals' subjective norms and risk perception also play crucial roles in shaping the U-shaped curvilinear relationship. Given the interaction between situational support and subjective norms, the U-shaped curvilinear relationship between situational support and risk perception remains when subjective norms is high, but insignificant when subjective norms are at a low level. This echoes existing research (Kasperson et al.,1988; van der Linden, 2015) that non-work users with a high level of subjective norms to information security, their risk perceptions of information security can be significantly enhanced with the increasing situational support, compared to those who have a lower level of subjective norms. The results also indicated that when situational support is at a moderate and a high level, the curvilinear relationship between situational support and ISBI is partly mediated by risk perception.

7. Conclusions

The importance of information security has been increasingly recognised at an extensive organizational and community level, with more resources being allocated to motivate individuals' ISBI. Understanding the influence of situational support on ISBI in different contexts is of great importance for information security research and practice.

7.1 Implications for research

First, this study presented cross-disciplinary research that verified the role of situational support in ISBI formalization in cross-contexts, based on the principles of COR and SET in the field of behavioural science. Studying ISBI from the resource perspective is a typical angle; to the best of our knowledge, this is one of the first studies to examine ISBI by adopting COR. This broadens the scope of studying behavioural information security in behavioural psychology and organizational behaviour

Second, we divided the users into non-work and work settings by characterizing their purpose and decision-making process under the framework of COR, finding that situational support has a different effect on ISBI between non-work and work users. Based on this cross-context study, we echo and empirically validate the arguments raised by Li and Siponen (2011) and Dang-Pham *et al*. (2013) that researching the formation mechanism of ISBI requires a holistic probe into different contexts and angles, thus providing context-sensitive insights into the information security literature.

Third, we enriched the interpretation boundary of situational support in the field of behavioural information security by comparing and contrasting linear and nonlinear relationships. The involvement of risk perception in the research model helped describe the formalization of the linear and nonlinear relationships between situational support and ISBI in different contexts. In addition, we indicate the role of situational support on ISBI via subjective norms from a resource investment perspective. Existing research such as Vedadi and Warkentin (2020) discussed a herd mentality as one type of avoidance behaviour from losses in the formation of ISBI. We found the positive angle of the subjective norm that is, individuals will evaluate whether invest resources to meet the expectations of the "important others". The validation of the moderating effect of subjective norms contributes to a better understanding of the effect of situational support on ISBI.

7.2 Implications for practice

Our study has important implications for information users in non-work and work settings. For non-work use, this research indicates that users who have a high-level risk perception tend to generate ISBI. Therefore, the government has an important role in raising public cyber security awareness. Some good practices include consistently communicating to the public via integrated media platforms that anyone can be a victim of cybercrime, and launching Cyber Security Awareness Campaigns that encourage individuals to take action to protect themselves (UK Home Office, 2018). The public should be given access to case education in different scenarios, so as to help them establish more sustainable information security behavioural habits (Hong & Furnell, 2021). Second, enterprises need to comply with information security laws and enact their corporate responsibilities; for instance, the users need to be informed of any possible information security threats when using applications, to improve their risk perception and security awareness. As situational support is found as one of the important predictors of ISBI for work use, the organization should take the responsibility to improve employees' effort-reward expectancy and organizational citizenship behaviour with a credible level of situational support. More concretely, the organization needs to commit to setting an information security agenda along with a culture of building information security. Some pragmatic practices include increasing the budget for information security support, providing resources necessary for taking information security measures (Warkentin *et al*., 2011), designing specialised information security courses, offering off-the-job training, setting information security job/management positions, providing technical support and consulting services, and

weaving information security guide into employee guidebook and daily communications via social media, newsletters, display materials (posters, leaflets..) etc. It is noted that procedural and distributive organizational justice should be factored in the implementation of any information security policy, practice and support, where relevant departments and managers are required to take responsibility to ensure that the situational support is adopted in a fair, transparent and user-friendly manner.

7.3 Limitations and future research

This study has the following limitations. First, although full-time university students can suitably represent the non-work users given they are commonly seen as victims of information security who are excessively exposed to the Internet, they could not access more types of information security threats and have few information resources to manage due to their age and social experiences. Moreover, this group could not cover all the possible non-work users' scenarios, this seemingly homogenous group may have varied ISBI due to their different demographic factors such as age. Therefore, the current study could be seen as a prototype for future studies that can be conducted in different age and occupational cohorts to better understand non-workers' attitudes in ISBI from a resource perspective. Second, although we discussed the cognitive and affective dimensions of risk perception we measured risk perception in a general way. In the future, we will consider these two dimensions in the operationalizations, so as to further improve the research reliability. Third, this research is constrained by the cross-sectional design and self-reported measures that may limit casual relationships and external validity. To address this concern, we suggest conducting a short-term longitudinal study and multi-source data including qualitative data to strengthen the causal relationships among key variables within the formation of ISBI.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

Anderson, C. L., and R. Agarwal. 2010. Practicing Safe Computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly* 34 (3): 614-644. doi:10.2307/25750694.

Asteriou, D., and S. G. Hall. 2011. *Applied econometrics*. New York: Palgrave Macmillan.

Barnard, C. 1938. *The Functions of the Executive*. Cambridge, MA: Harvard Press.

Blau, P. M. 1964. *Exchange and Power in Social Life*. New York: Wiley.

Boss, S. R., D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak. 2015. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS quarterly* 39 (4): 837-864. doi:10.25300/MISQ/2015/39.4.5.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34 (3): 523-548. doi:10.2307/25750690.

Chang, C. H., J. Xu, and D-P. Song. 2015. Risk analysis for container shipping: from a logistics perspective. *The International Journal of Logistics Management* 26 (1): 147-171. Doi:10.1108/IJLM-07-2012-0068.

Chen, Y. and Zahedi, F. M. 2016. Individual's internet security perceptions and behaviors: polycontextual contrasts between the United States and China. *MIS Quarterly* 40(1):205-222. Doi:10.25300/MISQ/2016/40.1.09.

Cuganesan, S., C. Steele, and A. Hart. 2018. How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology* 37 (1): 50-65. doi:10.1080/0144929x.2017.1397193.

D'Arcy J., A. Hovav, D. Galletta. 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 20 (1): 79-98. doi:10.1287/isre.1070.0160.

Dang, D., S. Pittayachawan, and M. Z. Nkhoma. 2013. Contextual difference and intention to perform information security behaviours: A protection motivation theory approach. *Australasian Conference on Information Systems*: 1-10. doi:10.13140/2.1.3668.8169

Dang, D., and S. Pittayachawan. 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security* 48:281-297. doi:10.1016/j.cose.2014.11.002.

DeJoy, D. M., L. J. Della, R. J. Vandenberg, and M. G. Wilson. 2010. Making work safer: Testing a model of social exchange and safety management. *Journal of Safety Research* 41: 163-171. doi:10.1016/j.jsr.2010.02.001.

Dhillon, G, Y. Talib, and W. N. Picoto. 2020. The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems* 21 (1): 152-174. doi:10.17705/1jais.00595.

Dinev, T., and Q. Hu. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J Assoc Inf Sys* 8 (7): 386-408. doi:10.17705/1jais.00133.

Fishbein, M., and I. Ajzen. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*, MA: Addison-Wesley.

Fornell, C., and D. F. Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18 (1): 39-50. doi:10.2307/3151312.

Furnell, S., and N. Clarke. 2012. Power to the people? The evolving recognition of human aspects of security. *Computers & Security* 31 (8):983-988. doi:10.1016/j.cose.2012.08.004.

Furnell, S., W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li. 2018. Enhancing security behaviour by supporting the user. *Computers & Security* 75 (JUN): 1-9. doi:10.1016/j.cose.2018.01.016.

Guo, K. H., Y. Yuan, N. P. Archer, and C. E. Connelly. 2011. Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems* 28 (2): 203-236. doi:10.2753/mis0742-1222280208.

Halbesleben, J. R., J. P. Neveu, S. C. Paustian-Underdahl, and M. Westman. 2014. Getting to the "COR" understanding the role of resources in conservation of resources theory. *Journal of Management* 40 (5): 1334-1364. doi:10.1177/0149206314527130.

Han, J, Y. J. Kim, and H. Kim. 2017. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security* 66 (MAY): 52-65. doi:10.1016/j.cose.2016.12.016.

Hayes, A. F. 2013. *An Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-Based Approach*. New York: Guilford Press.

Herath, T., and H. R. Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18 (2): 106-125. doi:10.1057/ejis.2009.6.

Hobfoll, S. E. 1989. Conservation of resources: A new attempt at conceptualizing stress. *American psychologist* 44 (3): 513-524. doi:10.1037/0003-066x.44.3.513.

Hobfoll, S. E. 2001. The influence of culture, community, and the nested-self in the stress process: Advancing conservation of resources theory. *Applied Psychology: An International Review* 50 (3): 337-421. doi:10.1111/1464-0597.00062.

Hobfoll, S. E. 2011. Conservation of resource caravans and engaged settings. *Journal of Occupational and Organizational Psychology* 84 (1): 116-122. doi:10.1111/j.2044-8325.2010.02016.x.

Hobfoll, S. E., J. Halbesleben, J. P. Neveu, and M. Westman. 2018. Conservation of resources in the organizational context: The reality of resources and their consequences. *Annual Review of Organizational Psychology and Organizational Behavior* 5 (1): 103-128. doi:10.1146/annurev-orgpsych-032117-104640.

Hofmann, D. A., and F. P. Morgeson. 1999. Safety-related behavior as a social exchange. *Journal of Applied Psychology* 84 (2): 286-296. doi:10.1037/0021-9010.84.2.286.

Home Office (2018) 'A Call to Action: the Cyberaware perceptions gap', Available from:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/684609/BT_CYBER_AWARE_V11_280218.pdf [Accessed: 09/01/2022]

Hong, W., and J. Y. L. Thong. 2013. Internet privacy concerns: an integrated conceptualization and four empirical studies. *MIS Quarterly* 37 (1): 275–298. https://www.jstor.org/stable/43825946

Hong, Y., and S. Furnell. 2019. Motivating information security policy compliance: Insights from perceived organizational formalization. *Journal of Computer Information Systems* 1-10. doi:10.1080/08874417.2019.1683781

Hong, Y., and S. Furnell. 2021. Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications* 57. doi:10.1016/j.jisa.2020.102710.

Hong, Y., J. S. Kim, and L. Xiong. 2019. Media exposure and individuals' emergency preparedness behaviors for coping with natural and human-made disasters. *Journal of Environmental Psychology* 63 (JUN): 82-91. doi:10.1016/j.jenvp.2019.04.005.

Hu, S., C. Hsu, and Z. Zhou. 2021. The impact of SETA event attributes on employees' security-related Intentions: An event system theory perspective. *Computers & Security* 109 (4): 102404. doi:10.1016/j.cose.2021.102404.

Huang, Y. H., J. Lee, A. C. McFadden, L. A. Murphy, M. M. Robertson, J. H. Cheung, and D. Zohar. 2016. Beyond safety outcomes: An investigation of the impact of safety climate on job satisfaction, employee engagement and turnover using social exchange theory as the theoretical framework. *Applied Ergonomics* 55: 248-257. doi:10.1016/j.apergo.2015.10.007.

IBM Corporation. 2021. *IBM X-force Threat Intelligence Index 2021*. Armonk, NY: IBM Security.

Ifinedo, P. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31 (1): 83-95. doi:10.1016/j.cose.2011.10.007.

Ifinedo, P. 2018. Roles of organizational climate, social bonds, and perceptions of security threats on IS security policy compliance intentions. *Information Resources Management Journal* 31(1): 53-82. doi:10.4018/irmj.2018010103.

Janssen, E., L. van Osch, L. Lechner, M. Candel, and H. de Vries. 2012. Thinking versus feeling: Differentiating between cognitive and affective components of perceived cancer risk. *Psychology & Health* 27: 767-783. doi:10.1080/08870446.2011.580846.

Johnston, A. C., M. Warkentin, and M. Siponen. 2015. An enhanced fear appeal framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* 39 (1): 113-134. doi:10.25300/MISQ/2015/39.1.06

Kasperson, R. E., O. Renn, P. Slovic, H. S. Brown, J. Emel, R. Goble, J. X. Kasperson, and S. Ratick. 1988. The social amplification of risk: A conceptual framework. *Risk Analysis* 8 (2): 177-187. doi:10.1111/j.1539-6924.1988.tb01168.x.

Kim, E. B. 2014. Recommendations for information security awareness training for college students. *Information Management & Computer Security* 22 (1): 115-126. doi:10.1108/imcs-01-2013-0005.

Kim, E. B. 2013. Information security awareness status of business college: Undergraduate students. *Information Security Journal: A Global Perspective* 22 (4): 171-179. doi:10.1080/19393555.2013.828803.

Kotulic, A. G., and J. G. Clark. 2004. Why there aren't more information security research studies. *Information & Management* 41 (5): 597–607. doi:10.1016/j.im.2003.08.001.

Lauver, K. J., S. Lester, and H. Le. 2009. Supervisor support and risk perception: Their relationship with unreported injuries and near misses. *Journal of Managerial Issues* 21 (3): 327-343. https://www.jstor.org/stable/40604653.

Li, H., J. Zhang, and R. Sarathy. 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems* 48 (4): 635-645. doi:10.1016/j.dss.2009.12.005.

Li, Y., and M. T. Siponen. 2011. A call for research on home users' information security behaviour. *Pacific Asia Conference on Information Systems*. https://aisel.aisnet.org/pacis2011/112

Liang, H., and Y. Xue. 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. *Journal of the Association for Information Systems* 11(7): 394-413. doi:10.17705/1jais.00232

Loewenstein, G., E. U. Weber, C. K. Hsee, and N. Welch. 2001. Risk as feelings. *Psychological Bulletin* 127 (2): 267-86. https://doi.org/10.1037/0033-2909.127.2.267

March, J. G., and H. A. Simon. 1958. *Organizations*. NewYork: Wiley.

Mearns, K. J., and T. Reader. 2008. Organizational support and safety outcomes: An un-investigated relationship. *Safety Science* 46: 388−397. doi:10.1016/j.ssci.2007.05.002.

Menard, P., G. J. Bott, and R. E. Crossler. 2017. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems* 34 (4): 1203-1230. doi:10.1080/07421222.2017.1394083.

Mitchell, V.W. 2005. Organizational risk perception and reduction: A literature review. *British Journal of Management* 6 (2): 115-133. doi:10.1111/j.1467-8551.1995.tb00089.x.

Mitnick, K. D. 2002. *The Art of Deception: Controlling the17 Human Element of Security*, New York: Wiley Publishing.

Moody, G. D., M. Siponen, and S. Pahnila. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly* 42 (1): 285-A222. doi:10.25300/MISQ/2018/13853.

Nagin, D. S., and G. Pogarsky. 2001. Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence. *Criminology* 39 (4): 865–891. doi:10.1111/j.1745-9125.2001.tb00943.x.

Ng, T. W. H., and D. C. Feldman. 2012. Employee voice behavior: A meta-analytic test of the conservation of resources framework. *Journal of Organizational Behavior* 33 (22): 216-234. doi:10.1002/job.754.

Ni, M., J.D. Mccalley, V. Vittal, T. Tayyib. 2007. Online risk-based security assessment. *IEEE Power Engineering Review* 22(11):59-59. doi:10.1109/TPWRS.2002.807091

Pérez-González, D., S. T. Preciado, and P. Solana-Gonzalez. 2019. Organizational practices as antecedents of the information security management performance: An empirical investigation. *Information Technology & People* 32 (5): 1262-1275. doi:10.1108/ITP-06-2018-0261.

Peters, E., B. Burraston, and C. K. Mertz. 2004. An emotion-based model of risk perception and stigma susceptibility: Cognitive appraisals of emotion, affective reactivity, worldviews, and risk perceptions in the generation of technological stigma. *Risk Analysis* 24: 1349-1367. doi:10.1111/j.0272-4332.2004.00531.x.

Peters, L.H., and E. J. O'Connor. 1980. Situational constraints and work outcomes: the influences of a frequently overlooked construct. *Academy of Management Review* 5 (3): 391-397. doi:10.5465/amr.1980.4288856.

Pluut, H., R. Ilies, P. L. Curşeu, and Y. Liu. 2018. Social support at work and at home: Dual-buffering effects in the work-family conflict process. *Organizational Behavior and Human Decision Processes* 146: 1-13. doi:10.1016/j.obhdp.2018.02.001.

Puhakainen, P., and M. Siponen. 2010. Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly* 34 (4): 757-778. doi:10.2307/25750704.

Renn, O., and E. Swaton. 1984. Psychological and sociological approaches to study risk perception. *Environmental International* 10: 557-575. doi:10.1016/0160-4120(84)90063-1.

Renn, O. 1998. The role of risk perception for risk management. *Reliability Engineering & System Safety* 59 (1): 49-62. doi:10.1016/s0951-8320(97)00119-1.

Safa, N. S., and R. V. Solms. 2016. Furnell S. Information security policy compliance model in organizations. *Computers & Security* 56: 70-82. doi:10.1016/j.cose.2015.10.006.

Settoon, R. P., N. Bennett, and R. C. Liden. 1996. Social exchange in organizations: perceived organizational support, leader-member exchange, and employee reciprocity. *Journal of Applied Psychology* 81 (3): 219-227. doi:10.1037/0021-9010.81.3.219.

Sharma, S., and M. Warkentin. 2019. Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security* 87: 101397. doi:10.1016/j.cose.2018.09.005.

Slovic, P., M. L. Finucane, E. Peters, and D. G. MacGregor. 2007. The affect heuristic. *European Journal of Operational Research* 177 (3): 1333-1352. https://doi.org/10.1016/j.ejor.2005.04.006

Snyman, D., and H. Kruger. 2019. Behavioural threshold analysis: methodological and practical considerations for applications in information security. *Behaviour & Information Technology* 38 (11): 1088-1106. doi:10.1080/0144929x.2019.1569163.

Sundblad, E. L., A. Biel, and T. Gärling. 2007. Cognitive and affective risk judgments related to climate change. *Journal of Environmental Psychology* 27: 97–106. doi:10.1016/j.jenvp.2007.01.003.

Taylor, A. B., D. P. MacKinnon, and J. Y. Tein. 2008. Tests of the three-path mediated effect. *Organizational Research Methods* 11 (2): 241-269. doi:10.1177/1094428107300344.

Thompson, N., T. J. McGill, and X. Wang. 2017. "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security* 70: 376-391. doi:10.1016/j.cose.2017.07.003.

Trumbo, C. W., L. Peek, M. A. Meyer, Marlatt, H. L., Gruntfest, E. , McNoldy, B. D., and Schubert, W. H. A cognitive-affect scale for hurricane risk perception. *Risk Analysis*, 2016, 36:2233-2246.

Tsai, H. S., M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotton. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security* 58: 138-150. doi:10.1016/j.cose.2016.02.009.

Tu, Z., O. Turel, Y. Yuan, and N. Archer. 2015. Learning to cope with information security risks regarding mobile device loss or theft: an empirical examination. *Information & Management* 52 (4): 506–517. doi:10.1016/j.im.2015.03.002.

Vance, A., M. Siponen, and S. Pahnila. 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management* 49 (3-4): 190-198. doi:10.1016/j.im.2012.04.002.

Vance, A., B. Anderson, C. B. Kirwan, and D. W. Eargle. 2014. Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems* 15 (10): 679-722. doi:10.17705/1jais.00375

van der Linden, S. 2015. The social-psychological determinants of climate change risk perceptions: Towards a comprehensive model. *Journal of Environmental Psychology* 41: 112–124. doi:10.1016/j.jenvp.2014.11.012.

van Schaik, P., D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev. 2017. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior* 75: 547-559. doi:10.1016/j.chb.2017.05.038.

Vedadi, A., and M. Warkentin. 2020. Can secure behaviors be contagious? A two-stage investigation of the influence of herd behavior on security decisions. *Journal of the Association for Information Systems* 21 (2): 428-459. doi:10.17705/1jais.00607.

Warkentin, M., A. C. Johnston, and J. Shropshire. 2011. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems* 20 (3): 267-284. doi:10.1057/ejis.2010.72.

Wason, K. D., M. J. Polonsky, and M. R. Hyman. 2002. Designing vignette studies in marketing. *Australasian Marketing Journal* 10 (3): 41-58. doi:10.1016/s1441-3582(02)70157-2.

Weber, E.U. 2006. Experience-based and description-based perceptions of long-term risk: Why global warming does not scare us (yet). *Climatic Change* 77: 103-120. doi:10.1007/s10584-006-9060-3.

Wolff, K., S. Larsen, and T. Øgaard. 2019. How to define and measure risk perceptions. *Annals of Tourism Research* 79:102759. doi:10.1016/j.annals.2019.102759.

Workman, M., W. H. Bommer, and D. Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior* 24 (6): 2799-2816. doi:10.1016/j.chb.2008.04.005.

Yukl G. 2002. *Leadership in organizations (5th Ed.)*. Upper Saddle River, NJ: Prentice-Hall.

Zajonc, R. B. 1980. Feeling and thinking: Preferences need no inference. *American Psychologist* 35: 151-175. doi:10.1037/0003-066X.35.2.151.

Zhen, J., Z. Xie, K. Dong, and L. Chen. 2022. Impact of negative emotions on violations of information security policy and possible mitigations. *Behaviour & Information Technology* 41 (11): 2342-2354. doi:10.1080/0144929x.2021.1921029.