Journal of Business Economics and Management
ISSN 1611-1699 / eISSN 2029-4433
2020 Volume 21 Issue 5: 1466–1485
https://doi.org/10.3846/jbem.2020.13169

POSITIVE EMOTIONS AND EMPLOYEES' PROTECTION-MOTIVATED BEHAVIOURS: A MODERATED MEDIATION MODEL

Jie ZHEN[1], Zongxiao XIE[2*], Kunxiang DONG[3]

[1]*School of Business Planning, Chongqing Technology and Business University, Chongqing, China*
[2]*China Financial Certification Authority, Beijing, China*
[3]*School of Management Science and Engineering, Shandong University of Finance and Economics, Jinan, China*

Received 25 November 2019; accepted 30 March 2020

Abstract. This study explores the relationship between positive emotions and protection-motivated behaviours by focusing on the mediating role of self-efficacy and the moderating role of information security awareness. Based on a sample of 215 full-time employees from various organizations in China, the results of hierarchical regression and moderated path analysis indicate that positive emotions positively influence protection-motivated behaviours, and self-efficacy partially mediates this relationship. In addition, information security awareness has a positive moderating effect on the relationships between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours. Furthermore, the findings show that information security awareness has a positive moderating effect on the mediating effect of self-efficacy between positive emotions and protection-motivated behaviours. The theoretical and practical implications of these results, as well as directions for future research, are discussed.

Keywords: protection-motivated behaviours, positive emotions, information security awareness, self-efficacy, protection motivation theory, broaden-and-build theory.

JEL Classification: D23, M54.

Introduction

With the wide application of information technology (IT) and information system (IS) in various industries, the important role of IT-related resources in promoting the development of organizations has been continuously illustrated in the past decade (Belanger et al., 2017; Shih & Yang, 2019). However, the frequent occurrence of information security incidents across several organizations has aroused public concern toward information security (Cram

*Corresponding author. E-mail: *xiezongxiao@vip.163.com*

et al., 2017). For example, 131,653 units of user data in www.12306.cn were leaked due to software bugs that were not fixed promptly in December 2014. Although external factors (e.g., hackers and spywares) pose a serious threat to the security of an organization's IT resources, organization employees' behaviours on information security are often viewed as a greater risk (Willison & Warkentin, 2013; Siponen et al., 2014; Johnston et al., 2016; Karjalainen et al., 2019). Despite numerous organizations adapting information security policies (ISPs), security issues originating from the non-compliant behaviours of employees have become an increasingly thorny problem for present day organizations (Johnston et al., 2015; Anderson et al., 2017; Khan & Alshare, 2019). Without employees' motivation to protect their organizations' IT resources (e.g., software, hardware and data), improving the effectiveness of organizations' ISPs is impossible (Lee et al., 2016).

Prior studies on information systems security (ISS) have shown that many organizations have incorrect or drastic understanding of information security management (Hwang & Cha, 2018; Cram et al., 2019). For example, several managers argue that information security cannot bring direct profit to organizations. Thus, organizations should not invest on activities related to ISS. In addition, other managers highlight that complying with the organizations' ISP inevitably reduces the efficiency of employees (D'Arcy et al., 2014). This one-sided view toward ISS leads to two types of security issues originating from employees' actions. On the one hand, employees' information security awareness is relatively deficient, which frequently results in the lack of sensitivity and initiative to understand organizational information security risks beyond the security requirements for reasonable and accurate coping procedures during information security incidents (Khan et al., 2011). On the other hand, employees lack basic information on security knowledge and are thus unarmed when addressing information security risks. As a result, employees' violations of ISP or the abuse or misuse of work computers frequently occurs within organizations (Niemimaa & Niemimaa, 2017). To this end, information security management at the organizational level should focus on cultivating employees' information security awareness and improving the self-efficacy level (Posey et al., 2013; Moody et al., 2018).

Collectively, prior studies on ISS have mainly examined the influence of various factors on employees' compliance or noncompliance of ISP using theories from the fields of psychology, sociology, and theoretical criminology (Cram et al., 2017). Although remarkable advances have been made in the literature, little attention has been given to employees' emotions and the positive emotions that organizations elicit to motivate employees to protect IT resources against external and internal threats. In particular, few studies have investigated how employees' emotions affect their protective security behaviours. Although employees' security-related behaviours are closely related to psychological movement (Burns et al., 2017), the existing studies mainly examine the influence of external factors (e.g., social norms and security regulations) on employees' information security behaviours (Cram et al., 2017; Burns et al., 2017). Thus far, little work has been carried out to explore the relationship between employees' internal emotions and their information security behaviours. To the best of our knowledge, only Gulenko (2014), Burns et al. (2017) and Burns et al. (2019) have discussed the positive emotions that can facilitate employees' information security behaviours. Second, despite the growing body of studies that have examined the nature of employees' compli-

ance or noncompliance toward ISPs (Siponen & Vance, 2010; Cheng et al., 2013), research on internal abilities and psychological factors that enable employees to proactively protect organizational information assets has remained nascent. Prior studies on employees' compliance to ISPs mainly discuss the organizational control measures that can effectively hinder their bad behaviours. In other words, the premise of these studies is that employees are unwilling to comply with ISPs. Conversely, this study argues that employees hold a positive attitude toward ISPs and are thus willing to adhere to ISPs and protect their organizations' information resources actively.

Accordingly, this study extends prior research by investigating the influence of positive emotions on employees' protection-motivated behaviours. Following Posey et al. (2013) and Posey, Roberts, and Lowry (2015), protection-motivated behaviours are defined as "volitional behaviours enacted by organization insiders to protect (1) organizationally relevant information and (2) the computer-based information systems in which the information is stored, collected, disseminated, and/or manipulated from information security threats". Moreover, given the significant role of positive emotions in motivating an individual's adaptive response and behaviour (Burns et al., 2017), this study argues that positive emotions may stimulate employees' protection-motivated behaviours efficiently. Hence, this study examines whether or not and how employees' positive emotions influence their protection-motivated behaviours. In addition, the current study explores the mediating role of self-efficacy and the moderating role of information security awareness in the relationship between positive emotions and protection-motivated behaviours.

This study aims to achieve three main objectives. First, this study tests the direct effect of positive emotions on protection-motivated behaviours. Second, this study examines the mediating effect of self-efficacy on positive emotions and protection-motivated behaviours. Third, this study explores the moderating effect of information security awareness on the relationships between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours. Therefore, this study builds and tests a moderated medication research model that considers positive emotions, self-efficacy, information security awareness, and protection-motivated behaviours.

The remainder of the paper is organized as follows. Section 1 reviews the theoretical foundation. Section 2 presents the research model and hypotheses. Section 3 introduces the methodology while the findings in this study is presented in Section 4. Section 5 demonstrates the discussion and conclusions which are critical for the implications, limitations and future study direction.

1. Theoretical background

1.1. Protection motivation theory

Protection motivation theory (PMT) is developed based on a series of studies on fear appeal. The theory was originally applied to the field of preventive medicine to explain individuals' proactive responses following the communication of health threats via fear appeals (Posey et al., 2015; Moody et al., 2018). Currently, PMT is widely considered a general theory of

motivation that can be used to explain individuals' behaviours toward any threat (Boss et al., 2015). PMT proposes that individuals respond to threats in an adaptive or maladaptive manner (Moody et al., 2018). Adaptive responses are actions that effectively minimize threats. In such cases, respondents use fear and threat as positive motivators for change. In contrast, maladaptive responses are actions that may help to reduce the fear resulting from a threat but fail to minimize the threat itself (Posey et al., 2015).

According to PMT, the protection motivation of an individual emanates from the process of threat appraisal and coping appraisal (Ifinedo, 2012). Threat appraisal is an individual's assessment of the level of danger posed by a threatening event, and it involves three factors, namely, perceived threat vulnerability, perceived threat severity, and potential rewards (Vance et al., 2012; Posey et al., 2014). Coping appraisal refers to an individual's evaluation of his or her ability to cope with a threat; this appraisal includes three factors, namely, response efficacy, self-efficacy, and response costs (Posey et al., 2015). Prior studies on ISS have indicated that PMT is useful and effective for predicting employees' information security behaviour within an organization (Johnston & Warkentin, 2010; Ifinedo, 2012; Vance et al., 2012; Posey et al., 2013; Siponen et al., 2014; Boss et al., 2015; Posey et al., 2015).

1.2. Broaden-and-build theory

With the rise of positive organizational behaviour, researchers have focused on the impact of positive emotions on employees' response and behaviours in the work environment (Burns et al., 2017). Broaden-and-build theory (BBT) offers a strong theoretical background for these studies. BBT describes the form and function of a subset of positive emotions (e.g., joy, contentment, and love), which can broaden an individual's thought–action repertoire and increase his or her ability to process information through a broadened scope of attention (Fredrickson, 2001). Conversely, negative emotions (e.g., anger and anxiety) always narrow individuals' mindsets (Beaudry & Pinsonneeault, 2010) and negatively influence their ability for learning and retaining memory (Gulenko, 2014).

After broadening employees' mindsets, positive emotions can improve performance through exploration or similar activities. Prior studies on positive psychology have indicated that positive emotions promote an individual's creative actions, ideas, and social bonds, which in turn build the individual's personal, intellectual, and social resources (Fredrickson, 2001). These resources can reinforce the possibility of successfully coping with information security issues with original ideas (Gulenko, 2014). Therefore, as employees increasingly seek to protect organizational information resources through creative IT-related activities, the effectiveness of the organization's ISPs will also substantially improve (Burns et al., 2019).

2. Research model and hypotheses

Building on the theories and studies discussed above, Figure 1 provides a research model. The model illustrates the relationship among positive emotions, self-efficacy, information security awareness, and protection-motivated behaviours. In addition, the model presents gender, age, educational level, industry type, and organization size as control variables. The research hypotheses will be elaborated and developed in the following sections.

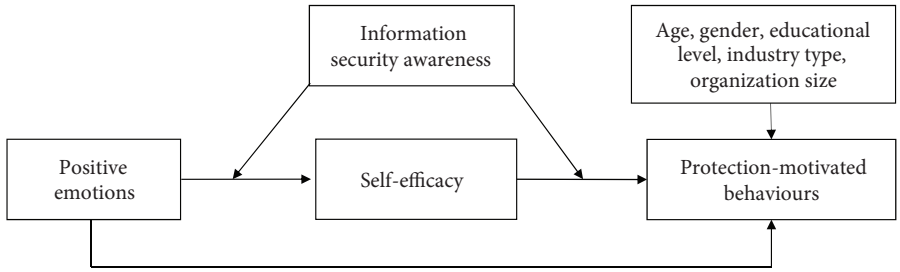

Figure 1. Research model

2.1. Positive emotions and protection-motivated behaviours

Prior studies have shown that positive emotions can enhance sociability, well-being, and constructive behaviour (Izard, 2002). Therefore, using positive emotions for the preventive intervention of negative incidents pertaining to information security within organizations is possible (Gulenko, 2014). Emotions have direct and indirect effects on employees' IT-related actions, and organizations should value employees' emotions in the workplace (Beaudry & Pinsonneeault, 2010). Positive emotions can promote employees' protection-motivated behaviours mainly in the following aspects. First, the social function of positive emotions is conducive for motivating employees to respect and accept the security requirement of the organization and to cooperate with others (Lazarus, 1991; Kaplan et al., 2013). This mindset is beneficial to the promotion of protection-motivated behaviours among employees. Second, the self-motivation function of positive emotions favours the stimulation of employees' positive self-assessment, such as happiness and satisfaction. In turn, employees are motivated to participate in the organization's information security management actively and spontaneously provide the energy necessary to protect the organization's information assets (Gulenko, 2014). In addition, prior empirical studies on moral emotions have shown that positive emotions are likely to guide employees in complying with the organization's moral codes and rejecting behaviours that violate the organization's rules (Hooge et al., 2011), which are beneficial for motivating employees' protection-motivated behaviours. Thus, it is posited that:

H1: Positive emotions are positively associated with protection-motivated behaviours.

2.2. Mediating role of self-efficacy

Positive emotions promote the construction of intellectual, interpersonal, and psychological resources, which enable employees to achieve a state of high energy activation, concentration, and pleasure (George & Zhou, 2007). For example, Bledow, Rosing, and Frese (2013) have argued that an increase in positive emotions typically result in employees' increased creativity. Beaudry and Pinsonneault (2010) have categorized positive emotions into challenge and achievement emotions and provided sound arguments that show how positive emotions are related to employees' exploration of new IT-related skills. The authors have also proposed that positive emotions can improve employees' knowledge and skills in IS research. Thus, the present study argues that positive emotions positively influence self-efficacy.

According to PMT, potential risk factors are involved in the work environment; employees will respond to such risk factors with either a good or a bad response, which is mainly dependent on their perception of risk factors and judgment of self-efficacy (Larose et al., 2008). By doing so, gaining a clear understanding of indicators and preventive measures when faced with information security risks is truly important for employees (Posey et al., 2015). In other words, self-efficacy is a prerequisite for directly determining whether employees implement protection-motivated behaviours. Thus, it is posited that:

H2: Self-efficacy mediates the relationship between positive emotions and protection-motivated behaviours.

2.3. Moderating role of information security awareness

Employees' information security awareness is a critical component that indicates whether an organization's information security management is effective (Bulgurcu et al., 2010). Thus, an increasing number of organizations carry out security education, training, and awareness (SETA) programs (Rezgui & Marks, 2008; Smith et al., 2010). Information security awareness can be described as a state in which employees are aware of the organization's security requirements. Particularly, this awareness focuses on the extent to which an employee understands the importance and implications of the policies, rules, and guidelines regarding information security management and the extent to which employees behave in accordance with these security requirements (Crossler et al., 2013).

As previously mentioned, positive emotions can stimulate employees' cognitive enthusiasm and proactive thinking and promote self-efficacy. Moreover, a high level of information security awareness can intensify the positive influence of positive emotions on employees' self-efficacy. In essence, employees armed with correct knowledge and attitude toward user privacy, customer data, and IT usage possess a high level of information security awareness (Dinev & Hu, 2007; Parsons et al., 2014). In other words, employees are inclined to generate positive emotions to improve self-efficacy further under the premise of high levels of information security awareness. In addition, employees with a high level of awareness can understand and be familiar with the security requirements within the organization in their daily work (Puhakainen & Siponen, 2010). These employees have a clear understanding of their responsibilities in terms of information security, which includes knowledge about sanctions when ISPs are violated (D'Arcy et al., 2009; Tsohou et al., 2013). In such circumstances, employees hold the appropriate attitude and understanding about information security management, and the relationship between self-efficacy and protection-motivated behaviours is reinforced. Thus, the following two hypotheses are posed:

H3: Information security awareness positively moderates the relationship between positive emotions and self-efficacy, such that positive emotions have a stronger positive impact on the self-efficacy of employees with higher levels of information security awareness compared with those with lower levels of information security awareness.

H4: Information security awareness positively moderates the relationship between self-efficacy and protection-motivated behaviours, such that self-efficacy has a stronger positive impact on the information security behaviour of employees with higher levels of information security awareness compared with those with lower levels of information security awareness.

2.4. Moderated mediation effects

As previously discussed, employees' positive emotions affect protection-motivated behaviours through the mediating effect of self-efficacy. However, the relationships between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours are intensified when employees possess high levels of information security awareness. Based on the two aspects, this study argues that information security awareness may moderate the mediating effect of self-efficacy on the relationship between positive emotions and protection-motivated behaviours. That is, a moderated mediating effect may exist.

Employees' high levels of information security awareness promotes the generation of positive emotions. Thus, employees tend to transform positive emotions into an increase in self-efficacy. Such an increase can also improve employees' ability to protect the information resources of their organizations. In contrast, when the level of employees' information security awareness is low, their positive emotions are suppressed. The stimulation of employees' self-efficacy substantially decreases, thus further reducing the possibility of information security protection. For example, several Chinese organizations provide training programs on information security awareness that emphasize that the main objective of security training is strengthening employees' acceptance of information security management. After a wide acceptance of information security management within the organization, the generation of positive emotions is more likely to increase, thus strengthening employees' self-efficacy and motivating protection behaviours by enforcing information security awareness. Thus, it is posited that:

H5: Information security awareness moderates the mediating effect of self-efficacy on the relationship between positive emotions and protection-motivated behaviours, such that the indirect effect of positive emotions on protection-motivated behaviours via self-efficacy is stronger for employees with high levels of information security awareness compared with those with low levels of information security awareness.

3. Research methodology

3.1. Measurement items

The measurement items for the constructs were developed based on prior studies. When available, this study directly used existing scales. In contrast, this study adapted closely related scales and adjusted such scales according to the context of the current research when unavailable. The questionnaire was verified using a two-step procedure. First, the content validity of measurement items was examined by two professors and one top manager who are familiar with information security management or instrument development. After refining the items based on their suggestions, this study distributed the questionnaire to 15 MBA students for validation. All measures used a five-point Likert-type scale, which was anchored from 1 = strongly disagree, 3 = neutral, and 5 = strongly agree.

Positive emotions were measured using the three-item scale adapted from Bhattacherjee (2001) and Beaudry and Pinsonneault (2010). Self-efficacy was measured using another three-item scale derived from Ifinedo (2014) and Johnston, Warkentin, and Siponen (2015).

Three-items for information security awareness were adapted from Bulgurcu, Cavusoglu, and Benbasat (2010) and D'Arcy, Hovav, and Galletta (2009). In the pretest, one item, namely, "I have sufficient knowledge about the cost of my organization's potential security problems" did not satisfy the requirement (its CITC value was 0.34, which was below 0.5). Thus, the item was omitted from the original version. Protection-motivated behaviours was measured with the three-item scale adapted from Posey et al. (2013) and Posey, Roberts, and Lowry (2015). Also, gender, age, educational level, industry type, and organization size were identified as control variables. Appendix Table A1 provides the measurement items for each construct.

3.2. Sample and data collection

The data used to test the research model were collected from a sample of full-time employees in China. With the help of several relevant industry associations and third-party certification authorities, this study distributed 300 electronic questionnaires through emails to employees in various organizations that implemented ISPs. To increase the generalizability of the result of the current study, the sample was selected to represent various educational levels and industry types. The respondents filled out the questionnaire based on their daily work experience. Finally, a total of 215 valid responses were collected with a valid response rate of 71.2%. Table 1 provides the demographics of the respondents.

Table 1. Demographics of respondents

Employee characteristics	Categories	Percentage (N = 215)
Gender	Male	57.7%
	Female	42.3%
Age	20–30	46.1%
	31–40	36.7%
	>40	17.2%
Education level	Polytechnic and below	7.9%
	Bachelor	51.2%
	Master's and PhD	40.9%
Industry type	Software	26.5%
	Financial services	35.4%
	Manufacturing	22.8%
	Telecommunications	15.3%
Organization size	<100	14.4%
	100–199	27.9%
	200–300	38.6%
	>300	19.1%

4. Data analysis and results

4.1. Measurement model

To assess the reliability of the measurement scale, Cronbach's alpha and composite reliability (CR) were evaluated. Table 2 shows that Cronbach's alpha values for all constructs were higher than the recommended threshold value of 0.7, whereas the CR of all constructs exceeded 0.8, which was more than the recommended score of 0.7. These values indicated positive reliability for all constructs.

Confirmatory factor analysis was used to evaluate convergent and discriminant validity. The loadings of each measurement item were higher than the recommended value of 0.7. In addition, all indicators in the analysis had higher loading values on corresponding constructs compared with other constructs (Table 3). These values suggest positive convergent validity for the measurement items of all constructs. In addition, Table 3 suggests that item loadings are higher than all cross-loadings. Furthermore, Table 4 shows that the square root of the average variance extracted for each construct is greater than the associated off-diagonal correlations. These results demonstrated discriminant validity.

Table 2. Loadings, CR, and AVE of measurement items

Construct	Measurement item	Loadings	AVE	CR	Cronbach's alpha
Positive emotions	PE1	0.84	0.71	0.88	0.79
	PE2	0.82			
	PE3	0.86			
Self-efficacy	SE1	0.88	0.72	0.88	0.82
	SE2	0.85			
	SE3	0.86			
Information security awareness	ISA1	0.88	0.76	0.91	0.84
	ISA2	0.88			
	ISA3	0.86			
Protection-motivated behaviours	PMBs1	0.88	0.73	0.89	0.82
	PMBs 2	0.87			
	PMBs 3	0.83			

Table 3. Cross-loadings

Constructs	Items	1	2	3	4
1. Positive emotions	PE1	0.84	0.42	0.60	0.45
	PE2	0.82	0.32	0.59	0.27
	PE3	0.86	0.49	0.65	0.34
2. Self-efficacy	SE1	0.39	0.88	0.46	0.61
	SE2	0.45	0.85	0.50	0.64
	SE3	0.44	0.86	0.51	0.67

End of Table 3

Constructs	Items	1	2	3	4
3. Information security awareness	ISA1	0.68	0.51	**0.88**	0.48
	ISA2	0.67	0.50	**0.88**	0.49
	ISA3	0.61	0.47	**0.86**	0.52
4. Protection-motivated behaviours	PMBs 1	0.40	0.66	0.50	**0.88**
	PMBs 2	0.37	0.69	0.52	**0.87**
	PMBs 3	0.34	0.55	0.43	**0.83**

Note: Values in bold indicate primary factor loadings.

4.2. Common method variance and multicollinearity check

In this study, a single questionnaire survey was used to collect data for all constructs at one point in time, which might lead to common method variance (CMV). This study used two steps to detect CMV. First, this study followed Bagozzi, Yi, and Phillips (1991) and Chen et al. (2018)'s research to test for potential CMV in our data. Table 4 shows that the correlations among all constructs in the present study are less than the suggested threshold of 0.9. This result demonstrated the absence of strong evidence of significant CMV. To ensure that this study is unaffected by CMV, this study further used Harman's one-factor test to conduct exploratory factor analysis. The results indicated that the first factor only accounted for 36.6% of the total variance, which was less than the suggested 40%. This value implied that CMV was not a major concern.

Table 4. Correlation analysis of latent variables

	Mean	Std.	1	2	3	4
1. Positive emotions	3.56	0.88	**0.84**			
2. Self-efficacy	3.58	0.95	0.50	**0.85**		
3. Information security awareness	3.42	0.98	0.75	0.57	**0.87**	
4. Protection-motivated behaviours	3.51	0.94	0.43	0.74	0.57	**0.86**

Note: Values in the diagonal area pertain to AVEs.

Multicollinearity was also a potential problem for the multi-regression analysis. Table 4 indicates that two correlation values of the four constructs are more than 0.6. Thus, this study needed to compute the variance inflation factor (VIF) to eliminate any potential threat of multicollinearity. The results revealed that the highest VIF was 1.86, which was less than the suggested 3.3. Therefore, multicollinearity was not a concern.

4.3. Test of hypotheses

This study used hierarchical linear regression (HLR) to test the research hypotheses. Prior studies on IS have indicated that HLR is frequently used to test models involving interaction effects (Chatterjee & Ravichandran, 2013; Chen et al., 2014). This type of analysis is appli-

cable to our study, as it aims to investigate the relationship among positive emotions, self-efficacy, information security awareness, and protection-motivated behaviours. In addition, using HLR to test for moderating effects can produce accurate estimates of the intensity of the interaction between variables (Rai & Tang, 2010; Chen et al., 2014).

Models 1 and 2 specify the impact of control variables and positive emotions, respectively, on self-efficacy. In Model 3, information security awareness and a multiplied moderating variable are added (i.e., positive emotions and information security awareness) based on Model 2. Models 4 and 5 present the impact of control variables and positive emotions, respectively, on protection-motivated behaviours. In Model 6, self-efficacy is added as an independent variable based on Model 5. Model 7 specifies the impact of control variables, independent variables, and interactions of the multiplied moderating variables on protection-motivated behaviours.

Table 5 shows the results of the regressions. In the test for direct effect, the data in Model 4 indicates that the effects of all control variables on protection-motivated behaviours are not significant. The explanatory power of this equation was also not significant. In Model 5, positive emotions have a positive effect on protection-motivated behaviours ($\beta = 0.357$, $p < 0.001$). Meanwhile, the value of ΔR^2 was $0.113 > 0$, which indicated that explanatory power considerably increased compared with Model 4. Thus, H1 was supported.

In the test for mediating effect, Model 5 indicates that the effects of all control variables are not significant. That is, positive emotions had a positive effect on information security behaviour ($\beta = 0.357$, $p < 0.001$). In Model 2, positive emotions have a positive effect on self-efficacy ($\beta = 0.430$, $p < 0.001$), whereas Model 6 indicates that positive emotions ($\beta = 0.213$, $p < 0.05$) and self-efficacy ($\beta = 0.669$, $p < 0.001$) have a positive effect on protection-motivated behaviours. Compared with the results of Model 5 and 6, the findings show that the regression coefficient has decreased significantly from 0.36 to 0.21. Therefore, positive emotions had a positive effect on protection-motivated behaviours through the mediating role of self-efficacy, which strongly supported H2.

Table 5. Results of regression analysis

	Self-efficacy			Protection-motivated behaviours			
	M1	M2	M3	M4	M5	M6	M7
Control variables							
Gender	0.11	0.06	0.07	0.11	0.04	−0.01	0.01
Age	0.10	0.09	0.09	0.02	0.01	−0.05	−0.05
Educational level	−0.01	0.03	0.06	0.03	0.06	0.03	0.04
Industry type	0.09	0.10	0.10	0.12*	−0.12	−0.07	−0.05
Firm size	0.07	−0.08	0.06	0.07	0.07	0.08	0.09
Independent variables							
Positive emotions		0.43***	0.40***		0.36***	0.22*	0.26*
Self-efficacy						0.67***	0.59***
Information security awareness			0.41***				0.19*

End of Table 5

	Self-efficacy			Protection-motivated behaviours			
	M1	M2	M3	M4	M5	M6	M7
Interaction							
Positive emotions × Information security awareness			0.27*				0.42**
Self-efficacy × Information security awareness							0.22**
R^2	0.15	0.31	0.44	0.15	0.26	0.57	0.60
ΔR^2	0.15	0.16	0.13	0.15	0.11	0.31	0.03
F	7.07	15.52	17.65	7.30	12.33	39.41	83.24

Note: *Significant at $p < 0.05$; **Significant at $p < 0.01$; ***Significant at $p < 0.001$.

In the test for moderating effect, Model 3 indicates that information security awareness has a positive moderating effect on the relationship between positive emotions and self-efficacy ($\beta = 0.264$, $p < 0.05$). Hence, H3 was supported. In Model 7, information security awareness has a positive moderating effect on the relationship between self-efficacy and protection-motivated behaviours ($\beta = 0.216$, $p < 0.05$). Thus, H4 was supported. In the follow-up test, this study used a simple slope test to examine the moderating effect of information security awareness further. Figure 2 shows a strong correlation between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours with high levels of information security awareness. In comparison, the correlation between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours was weak with low levels of information security awareness. These results indicated that with the improvement of the levels of information security awareness, the relationships between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours had been positively strengthened. Hence, H3 and H4 were further supported.

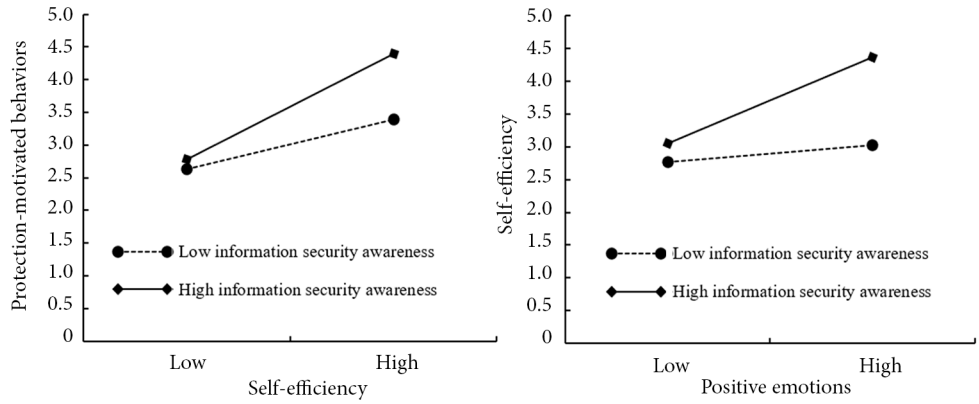

Figure 2. Analysis of moderated mediating effect

In the test for moderated mediating effect and following the recommendations of Edwards and Lambert (2007) and Pham, Tuckova, and Pham (2019), this study used the PROCESS macro for SPSS with 5,000 bootstrap samples at the 0.05 level to test H5 (Table 6). The results indicated that at high levels of information security awareness (i.e., mean + 1 SD), positive emotions had a considerable impact on protection-motivated behaviours through self-efficacy ($\beta = 0.325$, $p < 0.001$). At low levels of information security awareness (i.e., mean − 1 SD), positive emotions had a nonsignificant effect on protection-motivated behaviours through self-efficacy ($\beta = 0.058$, $p > 0.05$). The results indicated that with the improvement of information security awareness, positive emotions played an increasing important role in information security protection through self-efficacy, which strongly supported H5.

Table 6. Mediating effect under different levels of information security awareness

Information security awareness	Positive emotions (X) → Self-efficacy (M) → Protection-motivated behaviours (Y)				
	Stage		Effect		
	$X \rightarrow M$	M → Y	Direct	Indirect	Total
Lower (−1 SD)	0.06	0.06	0.10	0.06	0.16
Higher (+1 SD)	0.15*	0.16**	0.26**	0.33***	0.59**
Difference	0.09**	0.10**	0.16**	0.27**	0.43**

Note: *Significant at $p < 0.05$; **Significant at $p < 0.01$.

5. Discussion

This study provides important contributions to the literature on ISS in three ways. First, this study has found that positive emotions have a positive effect on protection-motivated behaviours, whereas self-efficacy has a mediating effect on this relationship. To the best of our knowledge, this study is one of the first to explore the links among these variables in the context of information security management. Our research model provides new insight into the critical role of positive emotions in employees' protection-motivated behaviours, which is a useful endeavour to construct a potential link between BBT and PMT. This study offers two new perspectives on PMT. We first concretized the relatively abstract construct of protection-motivated behaviours with specific content in the context of organizational information security management; we then showed that protection-motivated behaviours are the result of positive emotions. Therefore, this study opens up opportunities to extend PMT in the research on ISS by integrating emotion as a factor from the perspective of positive psychology.

Second, our analysis illustrates the important moderating roles of information security awareness between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours. These relationships have been developed based on the theoretical framework of PMT and BBT. Although the role of information security awareness in organization information security has been studied extensively, it is typically viewed as an important antecedent variable of individual security behaviour (Dinev & Hu,

2007; D'Arcy et al., 2009; Bulgurcu et al., 2010) and a dependent variable (Shaw et al., 2009; Ahlan et al., 2015). By verifying the moderating role of information security awareness, this study confirms that information security enhances the relationships between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours. These results are complementary to the role of information security awareness in the research on ISS.

Third, this study also contributes to BBT by showing the mediating role of self-efficacy between positive emotions and protection-motivated behaviours. Positive emotions have been extensively studied in the field of positive psychology. However, the application of research results regarding positive emotions is relatively limited. Applying such research results of positive emotions in the research on ISS not only verifies the application of positive emotions in information security but also enriches various links between factors of PMT by integrating PMT and BBT. Further, we posit that positive emotions are important drivers of both self-efficacy and protection-motivated behaviours. The empirical results support these arguments that extend BBT from an information security management perspective.

The findings also have several significant practical contributions. First, our study shows that positive emotions have a positive effect on protection-motivated behaviours. This result provides considerable guidelines for organizations with regard to the importance of employees' emotions. Thus, organizations should take action to influence employees' positive emotions. For example, when issue-specific security policies change in terms of new situations, employees may feel unsure about their knowledge or ability to comply with the policies, thus resulting in negative emotions. Accordingly, if the education and training programs provided by organizations can address this problem in this case, then the employees' positive emotions (e.g., happiness, excitement, and satisfaction) are stimulated. In response, employees are likely to adhere to security policies and protect the organization's information resources.

Second, our results confirm the mediating role of self-efficacy in the link between self-efficacy and protection-motivated behaviours. These results offer important implications for organizations that are truly concerned about employee actions in terms of security management. Accordingly, organizations should strive to equip employees with knowledge through security training and education programs. In particular, these programs should increase employees' self-efficacy level by explaining how to recognize security risks and cope appropriately. Therefore, whenever possible, organizations should enhance employees' belief toward information security and enrich security-related knowledge.

Third, the finding that information security awareness moderates the relationships between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours call for increased attention to training in relation to information security awareness. Therefore, organizations should convey the message that information resources are considerably important to the survival and development of employees. In addition, information behaviours that conform to ISP are crucial. Such concepts should be infiltrated and implemented into the daily work of each employee. In addition, organizations should continuously expand employees' knowledge and strengthen information security awareness through available means when certain rules and standards change.

Conclusions

Although researchers and practitioners have confirmed that employees' emotions and behaviours influence organizational information security, knowledge about how organizations improve the effectiveness of ISPs by motivating employees' positive emotions and protective behaviours is still emerging. Building on the extant literature, this study examines the roles of self-efficacy and information security awareness on the link between positive emotions and protection-motivated behaviours. Our results support the hypothesized links in the model. Our key findings are fourfold. First, positive emotions have a positive effect on protection-motivated behaviours. Second, self-efficacy mediates the relationship between positive emotions and protection-motivated behaviours. Third, the moderation hypotheses received support in that information security awareness moderates the relationships between positive emotions and self-efficacy and between self-efficacy and protection-motivated behaviours. Fourth, the findings also showed that information security awareness positively moderates the mediating effect of self-efficacy on the relationship between positive emotions and protection-motivated behaviours.

Three limitations to this study can guide future studies. The first is that data have been collected from organizations that implement ISP, which limits the industry type of the sample to a certain extent. Organizations in certain industries are likely to build connections with relevant industry associations and third-party certification authorities due to the high requirements for information security. This study developed a sample frame with this notion, which has inevitably resulted in insufficient coverage of the industry type of the study sample. Therefore, future studies should include data from various industries to validate the findings of the current study. Second, this study used a questionnaire to measure all constructs, and the singularity of the source may introduce CMV. Although the results show that CMV is not a major concern in this study, future studies can use objective data or data from multiple informants to enhance the accuracy of the empirical results. Finally, this study does not consider the influence of culture. Behavioural differences exist between employees across culture backgrounds, such as collectivist and individualistic cultures. For example, employees that come from a culture that emphasizes individualism may opt to place their personal interests first, whereas the opposite is true for employees with a collectivist mindset. This study has collected data from organizations in China, which tend to adapt the collectivist culture. Thus, future studies can address this limitation by collecting data from collectivist and individualistic cultures.

Acknowledgements

The authors thank the editor and reviewers for their comments and suggestions.

Funding

This research was supported by the National Natural Science Foundation of China, grant number 71802143.

Author contributions

Jie Zhen conceived the study and responsible for the design of the manuscript. Jie Zhen, Zongxiao Xie, and Kunxiang Dong were responsible for data collection and analysis. Kunxiang Dong were responsible for interpretation of results. Jie Zhen and Zongxiao Xie wrote the first draft of the manuscript. All the three authors agreed the final version of the article.

Disclosure statement

The authors declare no financial, professional, and personal interests from other parties.

References

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: Its antecedents and measures. *Procedia Computer Science*, *72*, 361–373. https://doi.org/10.1016/j.procs.2015.12.151

Anderson, C., Baskervill, R. L., & Kaul, M. (2017). Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems*, *34*(3), 1082–1112. https://doi.org/10.1080/07421222.2017.1394063

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly*, *36*(3), 421–458. https://doi.org/10.2307/2393203

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, *34*(4), 689–710. https://doi.org/10.2307/25750701

Belanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*(7), 887–901. https://doi.org/10.1016/j.im.2017.01.003

Bhattacherjee, A. (2001). Understanding information systems continuance: An expectation-confirmation model. *MIS Quarterly*, *25*(3), 351–370. https://doi.org/10.2307/3250921

Bledow, R., Rosing, K., & Frese, M. (2013). A dynamic perspective on affect and creativity. *Academy of Management Journal*, *56*(2), 432–450. https://doi.org/10.5465/amj.2010.0894

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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://www.jstor.org/stable/25750690

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190–209. https://doi.org/10.1016/j.chb.2016.11.018

Burns, A. J., Roberts, T. L., Posey, C., & Lowry, P. B. (2019). The adaptive roles of positive and negative emotions in organizational insiders' engagement in security-based precaution taking. *Information Systems Research*, *30*(4), 1228–1247. https://doi.org/10.1287/isre.2019.0860

Chatterjee, D., & Ravichandran, T. (2013). Governance of interorganizational information systems: A resource dependence perspective. *Information Systems Research*, *24*(2), 261–278. https://doi.org/10.1287/isre.1120.0432

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1409–1060. https://doi.org/10.1016/j.im.2018.05.011

Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., & Chow, W. S. (2014). IT capability and organizational performance: the roles of business process agility and environmental factors. *European Journal of Information Systems*, *23*(3), 326–342. https://doi.org/10.1057/ejis.2013.4

Cheng, L., Li, Y., Li, W., & Holm, E. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, 447–459. https://doi.org/10.1016/j.cose.2013.09.009

Cram, W. A., D'Arcy, J., & Proudfoot, J. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioural information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee response to stressful information security requirement: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

D'Arcy, Y. J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–88. https://doi.org/10.1287/isre.1070.0160

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. https://aisel.aisnet.org/jais/vol8/iss7/23

Edwards, J. R., & Lambert, L. S. (2007). Methods for integrating moderation and mediation: A general analytical framework using moderated path analysis. *Psychological Methods*, *12*(1), 1–22. https://doi.org/10.1037/1082-989X.12.1.1

Fredrickson, B. L. (2001). The role of positive emotions in positive psychology: The broaden-and-built theory of positive emotions. *American Psychologist*, *56*(3), 218–226. https://doi.org/10.1037/0003-066X.56.3.218

George, J. M., & Zhou, J. (2007). Dual tuning in a supportive context: Joint contributions of positive mood, negative mood, and supervisory behaviors to employee creativity. *Academy of Management Journal*, *50*(3), 605–622. https://doi.org/10.5465/amj.2007.25525934

Gulenko, I. (2014). Improving passwords: Influence of emotions on security behaviour. *Information Management & Computer Security*, *22*(2), 167–178. https://doi.org/10.1108/IMCS-09-2013-0068

Hooge, I. E., Nelissen, R. M., Breugelmans, S. M., & Zeelenberg, M. (2011). What is moral about guilt? Acting "prosaically" at the disadvantage of others. *Journal of Personality and Social Psychology*, *100*(3), 462–473. https://doi.org/10.1037/a0021459

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282–293. https://doi.org/10.1016/j.chb.2017.12.022

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. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Izard, C. E. (2002). Translating emotion theory and research into preventive interventions. *Psychological Bulletin*, *128*(5), 796–824. https://doi.org/10.1037/0033-2909.128.5.796

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. https://misq.org/catalog/product/view/id/1394

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

Johnston, A. C., Warkentin, M., Mcbride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231–251. https://doi.org/10.1057/ejis.2015.15

Kaplan, S., LaPort, K., & Waller, M. J. (2013). The role of positive affectivity in team effectiveness during crises. *Journal of Organizational Behavior*, *34*(4), 473–491. https://doi.org/10.1002/job.1817

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, *30*(2), 687–704. https://doi.org/10.1287/isre.2018.0827

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(5), 10862–10868. https://doi.org/10.5897/ajbm11.067

Khan, H. U., & AlShare, K. A. (2019). Violators versus non-violators of information security measures in organizations – A study of distinguishing factors. *Journal of Organizational Computing and Electronic Commerce*, *29*(1), 4–23. https://doi.org/10.1080/10919392.2019.1552743

Larose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, *51*(3), 71–76. https://doi.org/10.1145/1325555.1325569

Lazarus, R. S. (1991). Progress on a cognitive-motivational-relational theory of emotion. *American Psychologist*, *46*(8), 819–834. https://doi.org/10.1037/0003-066X.46.8.819

Lee, C., Lee, C. G., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60–70. https://doi.org/10.1016/j.cose.2016.02.004

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1–20. https://doi.org/10.1057/s41303-016-0025-y

Parsons, K., McCormac, A., Butavicious, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire. *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Pham, N. T., Tuckova, Z., & Pham, Q. P. T. (2019). Greening human resource management and employee commitment towards the environment: An interaction model. *Journal of Business Economics and Management*, *20*(3), 446–465. https://doi.org/10.3846/jbem.2019.9659

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Posey, C., Roberts, T. L., Lowry, P. B., & Bennett, R. (2013). Insiders' protection of organization of organizational information assets: Developing of a systematic-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, *37*(4), 1189–1210. https://doi.org/10.25300/MISQ/2013/37.4.09

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organization insiders. *Information & Management*, *51*(5), 551–567. https://doi.org/10.1016/j.im.2014.03.009

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

Rai, A., & Tang, X. (2010). Leveraging IT capabilities and competitive process capabilities for the management of interorganizational relationship portfolios. *Information Systems Research*, *21*(3), 516–542. https://doi.org/10.1287/isre.1100.0299

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7–8), 241–253. https://doi.org/10.1016/j.cose.2008.07.008

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Shih, T., & Yang, C. (2019). Generating intangible resources and international performance: Insights into enterprises organizational behaviour and capability at trade shows. *Journal of Business Economics and Management*, *20*(6), 1022–1044. https://doi.org/10.3846/jbem.2019.10513

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Siponen, M., Adam, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly*, *34*(3), 463–486. https://doi.org/10.2307/25750687

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2013). Managing the introduction of information security awareness programs in organizations. *European Journal of Information Systems*, *24*(1), 38–58. https://doi.org/10.1057/ejis.2013.27

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

Willson, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01

APPENDIX

Table A1. Measurement items

Construct	Item
Positive emotions	I feel happy thinking about protecting my organization's information resources.
	I feel excited thinking about protecting my organization's information resources.
	I feel satisfied thinking about protecting my organization's information resources.
Self-efficacy	I have the necessary skills to avoid ISP violations.
	I have the expertise to implement preventative measures against information security threats.
	I can enable security measures on my work computer or system independently.
Information security awareness	I understand my responsibilities as prescribed in the ISPs to enhance the information security of my organization.
	I am aware of potential security threats and their negative consequences.
	I understand the concerns regarding information security and the risks they pose in general.
Protection-motivated behaviours	I actively attempted to protect my organization's information resources.
	I tried to safeguard my organization's information resources from security threats.
	I purposefully defended my organization from information security threats to its resources.