Information Processing and Management 59 (2022) 102744

Contents lists available at ScienceDirect

Information Processing and Management

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

IS professionals' information security behaviors in Chinese IT organizations for information security protection

Xiaofen Ma

Faculty of Arts and Social Sciences, Communications and New Media, National University of Singapore, Singapore 117416, Singapore

ARTICLE INFO

Keywords:
IS professionals
Information security protective behaviors
Theory of planned behavior
Protection motivation theory
Organizational commitment

ABSTRACT

Continued integration of technology for the purpose of connecting and exchanging data with other devices and systems over the Internet exposes information security (IS) to growing risks. Organizations can thus achieve a strategic advantage by securing IS as a pivotal information and intelligence asset. This study examined ways of motivating IS professionals to protect information security from potential risks, drawing on the theoretical frameworks of protection motivation theory (PMT) and the theory of planned behavior (TPB) as well as work-related organizational antecedents (e.g., organizational commitment and job satisfaction). This paper proposes structural equation modeling (SEM) in R as a framework for exploring relationships among the variables and determining the overall data fit to the hypotheses. SEM is a multivariate technique which simultaneously executes both factor analysis and aspects of multiple regression in order to estimate interrelated relationships while also allowing path analytic modeling to be performed with latent, unobserved variables. Using 804 questionnaires with SEM analysis, we find support for the following predictors' associations: (a) information security attitudes and subjective norms, as constituents of TPB, significantly influenced information security protective behaviors; (b) the coping appraisals (self-efficacy and response cost) and threat appraisals (threat susceptibility and threat severity) of PMT were significantly predictive of information security protective behaviors; and (c) organizational commitment positively impacted information security protective behaviors. However, job satisfaction and perceived behavioral control as a construct of TPB were not associated with information security behaviors. The main theoretical contribution of this research is that the addition of organizational commitment allows the behavioral science model to offer a novel understanding of IS professionals' protection motivation and actual behaviors in the Chinese context. This study has several practical implications for organizations. In order to encourage IS professionals to follow protective security behaviors, organizations should set up the belief that a close relationship with subordinates plays a vital role in ensuring information security, improve IS employees' perception and cognition of their importance to the organization, constantly highlight the importance of information security protection, and emphasize the severe consequences of information security threats during trainings.

1. Introduction

The rapid advancement of information-based technologies and services (e.g., Internet of Things) in China has created heavy reliance on information security (IS) to protect the valuable organizational data these systems hold (Zhang et al., 2017). In Internet of

E-mail address: xiaofen.ma.01@u.nus.edu.

https://doi.org/10.1016/j.ipm.2021.102744
Received 23 March 2021; Received in revised form 17 August 2021; Accepted 25 August 2021
Available online 29 September 2021

Things (IoT), security refers not only to cryptography, secure communication, privacy assurance but also security professionals' protective behaviors. Information security relies on a highly efficient authentication and authorization system for accessing organizational databases that hold commercially valuable and sensitive personal information. Hence, it is also impacted by inside information breaches within organizations (Safa & Ismail, 2013). In IoT, most information is either personal or organizational, such as date of birth, location, and organizational budgets. This is one of the challenges of working with such sensitive data. Thus, IS professionals need to ensure that they take into account potential privacy vulnerabilities, security loopholes, and so on to provide cross-system security protection (Li et al., 2016). IS professionals are therefore at the forefront of the security concept.

The security of an organization's information is becoming more reliant on the actions of its IS experts skilled in collecting, analyzing, and utilizing data and responsible for protecting the users' data to which they have access (Albrechtsen & Hovden, 2009; Herath & Rao, 2009; Jang-Jaccard & Nepal, 2014; Posey et al., 2015). Safa et al. (2015) reported that a primary reason for IS security lapses is the fact that IS professionals are the most vulnerable link in the security chain. While their services are indispensable, they constitute a significant threat to the organization. For example, between March and October 2016, an information technology (IT) expert at Zhaopin, a well-known internet firm in China, sold more than 155,000 items of personal information from within the organization, including home addresses, work units, and salaries, to a Beijing-based technology company (Lu, 2017). This action resulted in severe consequences for the organization, including financial loss, reputational damage, and personal privacy infringement charges. Hence, it would be a beneficial approach for organizations to focus on the emergence of behavioral information security (Crossler et al., 2013) as organizational members' behaviors that influence the availability, confidentiality, and integrity of information security (Stanton et al., 2015).

There is surprisingly little research on information security protection in China despite the importance of protecting organizational information assets with the help of IS professionals. Most research on the topic has been limited to Western organizations. To what extent their information security reasoning can be extended to China, a country with a vastly different culture and institutional context, is yet to be determined. In 2019, the 135 listed IT organizations in China were generating 2.75 trillion Yuan in revenue from their information-based businesses, an increase of 12.5% from the end of 2018 (CAC, 2019). Chinese IT organizations provide an excellent area for information security research because they have adopted many information systems and are prone to tremendous threats to their information security. To date, research in the Chinese context has only found that certainty of formal sanctions toward deviant IS behaviors, as a means of formal social control, cannot fully explain IS protection; this is consistent with a prior study, which investigated IS violations from a rational choice perspective (Cheng et al., 2013; Siponen & Vance, 2012). The overall antecedents, structure, and interrelationships of protective information security behavior need to be explored in greater detail.

To address this research void and augment the field's understanding of IS professionals' performance of protective behaviors, this study focuses on insights from behavioral and attitudinal perspectives. The protection motivation theory (PMT) is a behavioral science theory originally established to predict and elucidate behaviors influenced by an individual's threat appraisal (how thrilling and severe a negative outcome is) and coping appraisal (how efficient the risk-eliminating behavior is). Researchers in the information security field also found the theory of planned behavior (TPB), a well-established behavioral science theory, useful for determining predictors of information security behaviors (Ajzen, 2002; Sommestad et al., 2014). TPB deems that behavior is determined by a set of beliefs grouped into attitudes, subjective norms, and perceived behavioral control (Sommestad et al., 2019). This study combines both theories to present a more thorough representation of the ways in which perceptual and attitudinal factors influence behavior.

Although earlier studies have tried to use research frameworks that integrated PMT and TPB with other constructs (e.g., Bulgurcu et al. 2010, Herath & Rao 2009, Lee & Larsen 2009), very few work-related factors that profoundly impact the performance of IS experts as employees have been considered in an organizational setting. Since researchers have indicated that both individual and organizational factors are worth discussing, behavioral researchers should not neglect the influence of job satisfaction and organizational commitment on security performance and the desire to safeguard IS resources (Chang et al., 2012; Mowday et al., 2013; Spector, 1985).

Thus, the stated learning aims to engender knowledge of protective information security behaviors in the Chinese IT industry by incorporating two behavioral science theories—PMT (self-efficacy, response cost, perceived severity, and perceived vulnerability) and TPB (attitude toward information security protection, perceived behavioral control, and subjective norms)—with work-related organizational factors (organization commitment and job satisfaction).

Section 2 of this paper defines the two fundamental theories and the hypotheses. These are then discussed in Section 3, which presents the quantitative methodological approach to examination and explanation. Section 4 discusses data analysis and the results of the measurement and structural models. We discuss the study's findings and contributions to theory and practice in Section 5. Sections 6 and 7 describe the study's limitations, discuss potential research avenues, and present a conclusion.

2. Theoretical foundation and hypothesis development

A critical requirement of IoT is that devices should be interconnected to complete specific tasks pertaining to sensing techniques, communication, information processing, and security protection (such as information confidentiality, transmission security, and privacy protection). Hence, IoT should be able to acquire, transmit, and process the information collected from IoT end-nodes such as sensors, gateways, and intelligent devices via networks to accomplish complex tasks (Li et al., 2016). Thus, it is expected that IoT should be able to prevent information security risks such as data breaches, unauthorized access, identity masquerade, and privacy leaks and provide robust security (Lize et al., 2014). It is especially important to design an effective security strategy to protect information against inside security threat at the service level.

Every organization has a varied mix of employees, management, partners, and complex infrastructure that makes handling inside IS

threats a daunting challenge (Roy Sarkar, 2010). The insider threat posed by IS professionals is more elusive and perplexing than any other security threat. IS professionals' deviant behaviors can lead to potential damage through loss of revenue, loss of reputation, and loss of intellectual property for organizations. Technical solutions do not suffice since insider threats are fundamentally a people issue. Therefore, a two-pronged approach consisting of social and organizational assessment is essential in facilitating the prediction of information security protective behaviors carried out by IS professionals and preempting inside data breaches. This will ultimately improve the organization's information security, and therefore survivability and resilience.

Individual activity evaluation is a complex issue, and multiple theoretical models have indeed been presented to address various elements of human behavior. The behavioral aspect of information security commended were numerous. The majority of the researchers used psychoanalytic theory such as protection motivation theory, concept of planned behavior, and other useful theories to investigate information security behavior. Furthermore, researchers investigated the impact of protection incentives on information security behaviors, concluding that an individual's personal compliance with corporate policies is influenced by their observed protection reasons (Shepherd et al., 2014).

PMT and TPB are seminal theories that have recently been shown to be efficacious in the information security field. Fig. 1 provides an overview of the conceptual model proposed in this section and later tested empirically. Building on this foundation and incorporating work-related factors relevant to the information security domain, the fundamental theoretical contributions are to parallel significant organizational perspectives with two behavior-intention theories and constructs to study how IS professionals' protective behaviors can be influenced. The model is then tested in a Chinese organizational context. An explanation of these additions follows.

2.1. *Work-related organizational factors*

Much research has focused on IS employees' association with organizational information security and its impact on protection motivational level and consequent workplace behavior. Effective information security also considers work-related efforts. Employees with high organizational commitment continue their membership because the organization's values, goals, culture, and initiatives align with their own (Herscovitch & Meyer, 2002; Meyer et al., 1993). Similarly, employees with a positive emotional state as a subjective value of performance satisfaction within the organization decrease turnover intentions (Kim & Mun, 2018).

The first factor, organizational commitment, a vital construct of work-related factors, is defined as members' identification with, feeling of obligation for, emotional attachment to, and involvement in a specific organization; this presents a strong positive association with desired organizational citizenship behavior (Mowday et al., 2013). Organizational citizens with high affective commitment perceive their organizational values and goals as congruent with their own, which means that success in one component creates success in the other (Posey et al., 2015). This is strategically significant for employees because of the potential benefits they get in return, measured by improved productivity and heightened perceived meaningfulness of work in the long run. By establishing organizational commitment strategies, organizations encourage desired employees by forging a psychological link between organization and member

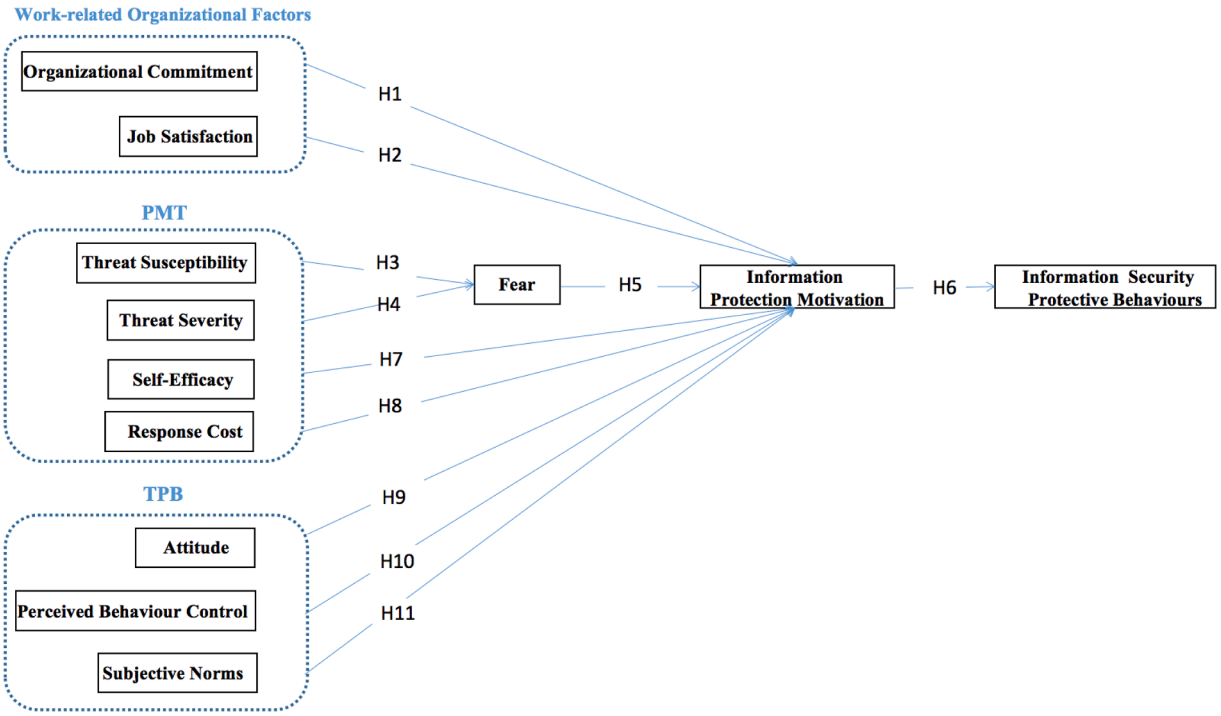

Fig 1. Theoritical Model.

expectations (Eisenhardt, 1985). Stanton et al. (2003) further developed a theoretical explanation for this link, documenting a positive association between organizational commitment and protective information security behaviors. The inference, then, in the context of information security protection, is that IS professionals, as organizational insiders with high levels of commitment, tend to exert considerable effort in performing and investing their knowledge and skills to protect their organizations' information security. In other words, organizational commitment can act as a predictive antecedent for IS professionals to trump information security threats and send a strong signal that information security protection is meaningful work. This leads to the first hypothesis:

H1: Organizational commitment is positively associated with IS protective motivation.

The second factor, job satisfaction, refers to an employee's sense of wellbeing at work. The construct is rather general, encompassing the employee's feelings about several job elements which can be intrinsic (i.e., relating to an employee's innate feelings of, for example, liking, happiness, or recognition) or extrinsic (i.e., referring to situational factors in an external setting such as pay, promotion, communication, supervision, rewards, and fringe benefits). Greene and D'Arcy (2010) state that IS professionals with positive feelings about their organizations and work are more likely to protect information assets and comply with information security procedures because they are closely involved in them and foresee the 'big picture' as far as their job responsibilities are concerned. Therefore, considering that this positive affect is reflected in job satisfaction, it is likely that more satisfied IS professionals engage in in-role information security performances that align with the corporate information security regulations that IT organizations expect and require. Previous studies have shown that the mutual association between levels of job satisfaction and job performance is rooted in social exchange theory, which proposes that individuals are more inclined to devote themselves to beneficial organizational behaviors if they are satisfied and perceive their employment relationship as a reciprocal exchange (Cheng et al., 2013; Podsakoff et al., 2003). Based on the above evidence, we postulate that higher job satisfaction may manifest itself in a stronger tendency towards information security protection. This leads to the second hypothesis:

H2: Job satisfaction is positively associated with IS protective motivation.

2.2. Protection motivation theory and research opportunities

In the information security field, PMT has been adapted to better understand the motivations that influence individuals to comply with organizational security policies and to employ anti-malware software (Johnston & Warkentin, 2010; Lee & Larson, 2009). The theory has also been used to explain various behaviors aimed at unified security practices (Anderson & Agarwal, 2010; Crossler & Bélanger, 2014) to protect computer and network security as well as adopt email authentication services (Herath et al., 2014). Even though many studies have relied on PMT in this context, its application and results have been inconsistent.

First, current research does not sufficiently consider the effects of fear despite its proof as an effective mediator by PMT scholars (Maddux & Rogers, 1983; Orazi & Pizzetti, 2015). Other studies omit fear entirely, mainly concentrating on other facets of PMT such as perceived severity and vulnerability, response cost, and self-efficacy (Ifinedo, 2012; Menard et al., 2018; Norman et al., 2005; Vance et al., 2012; Verkijika, 2018). However, a recent treatise on security research opportunities shows that fear has been acknowledged as a key PMT construct in theoretical reviews (Moody et al., 2018; Wall & Buche, 2017). For example, Herath & Rao (2009), studying behavioral information security, found that fear explains changes in information security attitudes toward security policy. Crossler et al. (2013) documented that fear should be delivered by emphasizing the information security threat's severity and the system's vulnerability. Notwithstanding contrary assumptions, existing research demonstrates that fear is an emotion with strong cognitive, affective, and psychological manifestations (Boss et al., 2015), which can substantially impact organizational members' security attitudes, motivations, behavioral intentions, and actual behaviors (Posey et al., 2015). Hence, omitting fear from PMT nomology may undermine IS research.

Second, although the primary purpose of PMT is to analyze protection motivation (i.e., intentions), it can be extended to assess actual protective behaviors associated with threat and coping appraisal. Previous information security studies employing PMT efforts have assessed actual protective information security behaviors (Lebek et al., 2013; Siponen et al., 2010), but most information security studies focus on protection motivation, which neglects the relation between protection motivation and actual behavior (e.g., Menard et al. 2018). Hence, this study argues that actual behaviors are useful for information security research because the goal is to improve security behavior, not merely to increase protection intentions. Further, comprehension of security practices in Chinese IT organizations depends on an efficacious test of IS professionals' actual behaviors that employs the full, inclusive nomology of PMT.

The threat and coping appraisal processes form the foundation of PMT. A threat appraisal consists of threat susceptibility—the degree to which IS professionals feel their organizations are susceptible to the described threat (Rogers, 1983)—and threat severity—the extent to which IS professionals perceive threats as detrimental and likely to cause consequential harm (Maddux & Rogers, 1983; Rogers, 1983). Belief in the existence of a harmful threat generates fear, a negative emotional response. Thus, threat vulnerability and severity predict fear. In the PMT model, researchers argued that fear, a significant component of the cognitive mediating process (Eppright et al., 2002), is generated as a partial mediator between threat appraisal and information security protection motivation. Invoking fear can lead an employee to take protective acts more seriously (Boss et al., 2015; Rogers, 1975; Witte, 1996). If information security protection motivation holds in the context of Chinese IT organizations, IS professionals' perceptions of security threats will impact the degree of fear they experience. This fear may influence their level of motivation to protect their organizations' information security from threats. It can also explain their engagement in protective responses in the future. Therefore, this study posits the following:

H3: Perceived threat susceptibility to the organizations' information security is positively associated with fear.

H4: Perceived threat severity to the organizations' information security is positively associated with fear.

H5: Fear related to organizations' information security threats is positively associated with IS protection motivation.

In the PMT model, it is well known that the primary theoretical focus predicts protection motivation intentions (Hassandoust & Techatassanasoontorn, 2020; Menard et al., 2018; Wu, 2020; Yoon & Kim, 2013). Further, Floyd et al. (2000) argued that PMT has been extended to predict behaviors. Therefore, PMT-centered research in the field of health is now used to examine real-world behavior change as well as behavioral intentions. In line with this reasoning, actual information security protective behaviors can be useful for information security research because the purpose is to change the actual security behaviors of IS professionals. To increase application to security practice, therefore, any test of the full nomology of PMT should contain an assessment of actual protective behaviors. Nevertheless, protection motivation (i.e., intention) as the key construct of the PMT model can be a very strong predictor of behaviors. Thus, we hypothesize as follows:

H6: IS protection motivation is positively associated with information security protective behaviors.

Coping appraisal involves the evaluation of one's ability to avoid and cope with threats to 'avert the threatened danger' (Floyd et al., 2000, p. 410). The process considers the two variables of self-efficacy and the cost of performing the protective behavior (i.e., response cost).

Self-efficacy is the assessment of one's capacity for protective behavior—whether the individual has the skills, experience, and instruments required to execute the work responsibly (Maddux & Rogers, 1983). Previous studies have always applied the concept to explain people's behavioral intentions while using computers (Crossler et al., 2013; Johnson & Marakas, 2000). PMT research has had similar results when employing self-efficacy to explain the performance of information security tasks. For example, Johnston and Warkentin (2010) found a direct positive relationship between self-efficacy and the use of anti-spyware software. Similarly, other researchers found a positive relationship between self-efficacy and attitudes toward the security of a home wireless network (Anderson & Agarwal, 2010; Woon et al., 2005). Therefore, we arrive at the following hypothesis:

H7: Self-efficacy is positively associated with protection motivation.

Finally, response cost refers to perceived personal drawbacks, such as the effort, expense, difficulties, inconveniences, and potential side effects that IS professionals believe they will incur from taking protective actions (Pratt et al., 1992). Workman et al. (2008) commented that 'people maintain different cost/benefit attitudes about information security measures that are independent of the perceived business value or sensitivity of the informational assets (i.e., severity of threat), particularly in relation to their own self--interests' (p. 2806). When response cost increases, the likelihood that IS professionals will perform adaptive responses decreases (Pechmann et al., 2003). IS research has found support for similar findings associated with/ in regard to the intention of using security measures (Hsu & Kuo, 2003; Workman et al., 2008; Wu & Wang, 2005).

H8: Response cost is negatively associated with protection motivation.

2.3. The theory of planned behavior and protection motivation

The second approach to information security from the perspective of protective intentions and behaviors draws upon TPB. Developed from the theory of reasoned action (TRA), TPB describes behavior changes from the perspective of social influence. In organizations, individuals' feelings, actions, and behaviors are influenced by their interaction with others. Evaluation of a behavior as positive (attitude) or performance of recommended behaviors as expected by significant others (subjective norms) may result in greater intention to perform the behavior (Fishbein & Ajzen, 1981). Ajzen (2002) went on to develop TPB by adding perceived behavioral control. From protective behavior intention to actual behavior, the theory can comprehensively elucidate nonvolitional behavior, postulating that individual behavior is influenced by attitude, subjective norms, and perceived behavioral control. Earlier studies demonstrated that a person's intention to support information security protection is strongly affected by these three factors (Bulgurcu et al., 2010). This research used TPB to explain how IS professionals engage in information security protection to decrease threats in organizations. The three constituents of TPB used in this study are explained below.

Attitude describes an individual's positive or negative view toward performing a specified behavior (Safa & Von Solms, 2016). Because of its great potential to describe a person's behavior, attitude has attracted researchers' attention in several research domains. For example, Siponen et al. (2014) pinpointed that attitude relates positively to compliance with organizational information security policies and that it impacts employees' intention to comply with security policies. This study postulates that a positive attitude toward information security protection has a positive effect on IS protection motivation.

H9: Attitude towards information security protection is positively associated with IS protection motivation.

Perceived behavioral control refers to individuals' perception of the ease or difficulty of performing the behavior. The ability or inability to perform the recommended behaviors influences an individual's own belief about intentions and relevant actions (Cox, 2012; Safa & Von Solms, 2016). Hence, the following hypothesis is proposed:

H10: Perceived behavioral control is positively associated with IS protection motivation.

Subjective norms are defined as the perception of what significant others think about a recommended behavioral pattern. They indicate the social pressure on organizational members to perform or refrain from performing a particular behavior (Cheng et al., 2013). In IT organizations, the social pressure comes from managers, team leaders, colleagues, and even subordinates who perceive information security protective motivation as an effective and important step that increases security awareness and decreases threats such as data breaches. Hence, we hypothesize the following:

H11: Subjective norms are positively associated with IS protection motivation.

3. Research methodology

3.1. Data collection and sample

To collect data, an online survey was administered by www.wjx.com (the largest online data collection platform in China) in September 2019. A reminder was distributed electronically one week later. Then, a pretest (n=25) was conducted to assess logical consistency, ease of understanding the wording of the questions, and contextual relevance of the measures to eliminate ambiguity.

Between September 2019 and October 2019, a total of 824 questionnaires were returned. Out of these, 20 questionnaires (2.4%) were omitted for being incomplete or having the same answer for every question. Therefore, 804 valid questionnaires remained.

Of the 804 valid participants, 56.9% were male and 43.1% female. Of all the participants, 71.1% had tenures in the IT industry ranging from 3 to 5 years or 5 years or above. More than 90% had a bachelor's degree or higher educational qualifications. As Table 1 shows, the participants' demographic data display diversity in terms of working experience, education, age, and gender.

3.2. Development of measures

All measures were based on the 7-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree).TPB constructs (i.e., attitude, perceived behavioral control, and subjective norms), PMT constructs (i.e., self-efficacy, response cost, threat susceptibility, threat severity, and fear), work-related organizational factors (i.e., organizational commitment and job satisfaction), and the dependent variable (IS protection-motivated behaviors) were measured by adapting pre-validated scales in order to minimize measurement risk. For TPB variables, IS attitude was measured with scales adapted from Safa et al. (2015). Perceived behavioral control and subjective norms were measured with scales adapted from Sommestad et al. (2014) and Ifinedo, 2012, respectively. For PMT factors, self-efficacy, response cost, and threat severity were measured with scales adapted from Workman et al. (2008). Fear was measured with scales adapted from Block and Keller (1995). Threat susceptibility was assessed with scales adapted from Johnston and Warkentin (2010). Protection motivation and protection-motivated behaviors were assessed with scales adapted from Posey et al. (2015).

For work-related organizational constructs, scales of organization commitment were adapted from a study conducted by Meyer and Allen (1997). Scales of job satisfaction were adapted from a study by Cammann et al. (1983). Table 2 provides a summary of the measurement scales, with 47 items in a concise form.

4. Results

Structural Equation Modeling (SEM) is recommended to explore complex relationships among latent variables (Holbert & Stephenson, 2003). The foremost suitable technique for discovering relationships between the variables then the entire information fit towards the theory is SEM. It detaches the error at the time of it estimates the latent factors along with the analyzed factors then the measurement deterioration betwixt the latent factor. SEM was performed in R using Lavaan, and it took one week to run data in October 2019. First, a full measurement model with all latent variables was tested by confirmatory factor analysis. The structural

Table 1
Participants' demography.

Demography	Category	Frequency	Percent (%)
Gender	male	458	56.9
	female	346	43.1
Age	18–25	67	8.3
	26–30	301	37.4
	31–40	407	50.6
	41–50	7	.87
	51–60	15	2.83
Education Level	High school or below	3	.37
	Bachelor degree	546	67.9
	Master degree	239	29.7
	Ph.D. degree	16	2.03
Monthly Salary	0–8000RMB	142	17.7
	8001–15000RMB	460	57.2
	15001–25000RMB	179	22.3
	25001RMB	23	2.8
Firm Size	20 or below	47	5.9
	21–50	385	47.9
	51–100	265	33.0
	100 or above	107	13.2
Tenure	1year or below	7	.9
	1–3years	224	27.9
	3–5years	287	35.8
	5 years or above	286	35.4

Note: RMB is abbreviation for Ren Min Bi (People's notes), which is the official currency of China.

Table 2
The measurements, items and their descriptive statistics.

Measurements		Items	Item Loading
Attitude	1	My Information security protective behaviour for users is necessary	.783
Safa et al.(2015)	2	Practicing information security protective behaviour for users is useful	.864
	3	I have a positive view about changing users' information security behaviour to conscious care	.796
	4	I believe that information security protective behaviour for users is valuable in their data protection	.851
Perceived Behavioural Control	1	I deem that information security protective behaviour is not a difficult practice	.851
Sommestad et al. (2014)	2	Information security protective behaviour is an achievable practice	.871
	3	I am certain that I can adhere to the information security protection behaviour at organization	.849
			.804
Subjective Norms	1	My manager thinks that I should protect information assets security	.827
Ifiendo (2012)	2	My colleagues think that I should protect information assets security	.658
	3	My organization's IT department pressures me to protect information assets security	.789
Self-Efficacy	1	I have the skills to protect my work-related data and users' private data	.850
Workman et al.(2008)	2	I have the necessary skills to protect my organization's information users' private data from information security violations	.867
	3	I think the protection of users' data is in my control in terms of information security violations	.881
	4	I have the ability to prevent information security violations	.880
Response Cost	1	The inconvenience to implement recommended security measures to protect my organization's information and information systems exceeds the potential benefits.	.827
Workman et al.(2008)	2	There are too many overheads associated with complying with information security measures	.867
	3	Using with information security measures would require considerable investment of effort other than time	.848
	4	The negative side effects of recommended security measures in my organization are greater than the advantages.	.843
Threat Severity	1	Threats to the security of my organization's information and information systems are severe.	.868
Workman et al.(2008)			
	2	I believe that threats to the security of my organization's information and information systems are serious.	.897
	3	I believe that threats to the security of my organization's information and information systems are significant.	.855
Threat Susceptibility	1	My organization's information and information systems are vulnerable to security threats	.870
Menard et al.(2018)	2	It is likely that the potential information security violation will occur to my organization's information and information systems	.877
	3	My organization's information and information systems are at risk to information security threats	.876
Fear		When thinking about the security threats to your organization's information and information systems, to what extent do you feel …?	
Block and Keller (1995)	1	Nervous	.842
	2	Anxious	.826
	3	Uncomfortable	.785
	4	Tense	.847
	5	Frightened	.795
Organizational Commitment	1	I would be very happy to spend the rest of my career with this organization	.812
Meyer and Allen (1997)	2	I really feel as if this organization's problems are my own	.802
	3	I do feel "emotionally attached" to this organization	.778
	4	This organization has a great deal of personal meaning for me	.806
Job Satisfaction	1	I would be very happy to spend the rest of my career with this organization	.852
Cammann et al.(1983)	2	I really feel as if this organization's problems are my own	.853
	3	This organization has a great deal of personal meaning for me	.802
	4	All in all, I am satisfied with my job	.858
Protection Motivation	1	I intend to protect my organization from its information security threats	.854
Posey et al.(2015)	2	My intentions to prevent my organization's information security threats from being successful are high	.858
	3	It is likely that I will engage in activities that protect my organization's information and information systems from security threats	.851
	4	I intend to expend effort to protect my organization from its information security threats	.853
	5	I intend to try my best to prevent information security threats from happening in my organization	.813
Information security behaviour	1	I actively attempt to protect my organization's information, users' private data and prevent information systems threats	.808
Posey et al.(2015)	2	I try to safeguard my organization's information, users' private data and computerized information systems from their information security threats	.843
	3	I take committed action to prevent information security threats to my firm's information, users' private data and computer systems from being successful	.856
	4	I purposefully defend my organization from information security threats to its information, users' private data and computerized information systems	.876
	5	I immediately report a co-worker's negligent information-security behaviour to the proper organizational authorities	.843

model was the focus of the second stage, which looked at the hypothesized connections between the components in this study. SEM was considered the utmost appropriate technique for the stated sort of research.

4.1. Assessment of measurement model

To assess the measurement model, reliability, convergent validity, and discriminant validity are usually evaluated. In this study, first, evaluate the reliability by checking the reliability of the components. By utilizing Cronbach's alpha, the reliability else accuracy of the estimation can be resolved (Cronbach & Shavelson, 2004). The reliability of entire structures exceeds .70, which is a usually utilized threshold (Peterson, 2014). The numerical value is betwixt .761 and .928, both of which above .70, which is illustrated in Table 3 as the outcome which indicates the sufficient reliability. Secondly, two criteria are utilized to evaluate convergence validity: (a) the loading of all items should be greater than the reference point .60; (b) the extracted average variance (AVE) should exceed the .50 threshold. It can be seen from Table 3 that the load of all items is greater than .60; in addition to, the AVE value exceeds .50. Therefore, our dimension model has respectable convergence validity. Third, the validity of the discrimination is guaranteed at the time of the following circumstances are met: (a) The value of AVE is higher than the threshold .50; (b) The square root of AVE is greater than all other cross-correlations. Table 3 shows the range of AVE from .516 to .731. In Table 4, there is no correlation between structures greater than the square root of AVE (the main diagonal element). By summarizing the outcomes, it ensures that the above specified estimations are applicable to this research.

4.2. Assessment of structural model

Next, the whole model was tested via SEM in R. First, we evaluated the research model's global goodness-of-fit. A good model should have a root mean square error of approximation (RMSEA) <.06, a comparative fit index (CFI) >.95, Tucker Lewis Index (TLI) >.95, and a standardized root mean square residual (SRMR) <.08 (Hu & Bentler, 1999). In our study, the results showed an excellent approximate fit for the research model: RMSEA = .036 (90% C.I. = .034, .038), CFI = .963, TLI = .959, and SRMR = .045. The chi-square statistics were significant ($\chi 2$ (1014) = 1888.041, p < .001). Also, we examined the significance of each hypothesized path, the results of which are summarized in Table 5.

4.3. Variables predicted information security behaviors

As Fig.2 shows, the results supported most of the hypotheses except for job satisfaction (H2) and perceived behavioral control (H10).

As for work-related organizational factors, organizational commitment (H1, $\beta = .112$, $p < .01$) was positively associated with information protection motivation. However, another organizational factor, job satisfaction (H2, $\beta = .074$, $p > .05$) was not significantly associated with information security protection motivation. Interestingly, this finding contradicts previous research results (Fatimah et al., 2011; Oplatka, 2009), which found that job satisfaction, as a factor of organizational psychology, was related to organizational citizenship behavior and could be significant in creating a better organization.

For protection-motivated factors, the threat appraisal components, threat susceptibility (H3, $\beta = .309$, $p < .001$) and threat severity (H4, $\beta = .357$, $p < .001$), had positive associations with fear. Taken together, the results suggest that threat appraisal evokes fear. Similarly, fear (H5, $\beta = .082$, $p < .05$) has been proved to have a positive association with information security protection motivation. Conversely, Posey et al. (2015) found that organization insiders are not generally motivated by fear and threat characteristics because 'attempting to scare insiders about potential threats through messages that specifically attempt to elicit fear might be ineffective in organizations' (p.33). A possible explanation is that for IS professionals, the subjects of this research, fear is a main security control that

Table 3
Measurement model reliability of latent variables.

Constructs	Number of Indicators	CR	AVE	CA
ATT	4	.887	.662	.886
PBC	3	.908	.713	.908
SN	3	.761	.516	.840
SE	4	.916	.731	.925
FA	5	.914	.680	.913
RC	4	.910	.717	.909
TSUS	3	.784	.549	.860
TSEV	3	.802	.575	.907
OC	4	.879	.646	.876
JS	4	.888	.665	.906
PMT	5	.928	.721	.928
ISPB	5	.926	.716	.926

Notes: 1.ATT = Attitude, PBC = Perceived Behaviour Control, SN = Subjective Norms, SE = Self-Efficacy, FA= Fear, RC = Response Cost, TSUS = Threat Susceptibility, TSEV = Threat Severity, OC = Organizational Commitment, JS = Job Satisfaction, PMT = Protection Motivation Theory, ISPB = Information Security Protective Behaviours
2. CR = Composite Reliability, AVE = Average Variance Extracted, CA = Cronbach's Alpha

Table 4
Correlations between main variables and the square root of the AVEs.

	Mean	SD	1	2	3	4	5	6	7	8	9	10	11	12
ATT	3.75	1.09	**.814**											
PBC	3.32	1.10	.482	**.844**										
SN	3.65	.99	.357	.454	**.718**									
SE	3.53	1.19	.390	.427	.502	**.855**								
FA	3.74	1.06	.436	.514	.446	.501	**.823**							
RC	4.15	1.08	-.409	-.480	-.444	-.419	-.471	**.846**						
TSUS	3.70	.90	.398	.452	.492	.561	.475	-.471	**.740**					
TSEV	2.65	1.16	.416	.464	.527	.533	.498	-.422	.495	**.758**				
OC	3.74	.88	.396	.402	.360	.428	.472	-.435	.378	.422	**.879**			
JS	3.70	.79	.407	.453	.431	.496	.521	-.475	.452	.512	.422	**.815**		
PMT	3.84	1.08	.422	.474	.411	.428	.444	-.435	.447	.418	.409	.427	**.849**	
ISPB	3.62	.94	.410	.453	.416	.447	.426	-.391	.380	.434	.364	.474	.371	**.846**

*Notes:*1. SD = Standard Deviation, ATT = Attitude, PBC = Perceived Behaviour Control, SN = Subjective Norms, SE = Self-Efficacy, FA= Fear, RC = Response Cost, TSUS = Threat Susceptibility, TSEV = Threat Severity, OC = Organizational Commitment, JS = Job Satisfaction, PMT = Protection Motivation Theory, ISPB = Information Security Protective Behaviours
2. The bold entries show the square root of the AVE (Average Variance Extracted)

Table 5
Hypotheses testing.

Hypotheses	β	T-value	P-value
H1: Organizational commitment → Protection Motivation	.122	2.903	**
H2: Job Satisfaction → Protection Motivation	.074	1.098	Not Supported
H3: Threat Susceptibility → Fear	.309	8.874	***
H4: Threat Severity → Fear	.357	10.161	***
H5: Fear → Protection Motivation	.082	2.381	*
H6: Protection Motivation → Information Security Protective Behaviours	.401	11.807	***
H7: Self-Efficacy → Protection Motivation	.086	2.233	*
H8: Response Cost → Protection Motivation	-.103	-2.500	*
H9: Attitude → Protection Motivation	.133	3.446	**
H10: Perceived Behavioural Control → Protection Motivation	.066	4.068	Not Supported
H11: Subjective Norms → Protection Motivation	.113	2.441	*

Note: * = *P*-value < .05; ** = *P*-value < .01; *** = *P*-value < .001

paints them as protectors of information assets. Their awareness of security threats and knowledge of the relevant severe consequences are stronger than those of ordinary organizational employees. Next, information security protection motivation (H6, $\beta = .401$, $p < .001$) was positively associated with protection-motivated behaviors.

As for coping appraisals of protection motivation model, self-efficacy (H7, $\beta = .086$, $p < .05$) was positively associated with information security protection motivation. Response cost (H8, $\beta = -.103$, $p < .01$) was positively associated with information security protection motivation.

As predicted, two out of the three constructs of TPB, attitude (H9, $\beta = .133$, $p < .001$) and subjective norms (H11, $\beta = .113$, $p < .05$) were positively associated with information security protection motivation. However, perceived behavioral control (H10, $\beta = .066$, $p > .05$) was not positively associated with information security protection motivation. This result is inconsistent with previous research. For example, analysis of partial correlations shows that attitude and perceived behavioral control have significant correlations with behavior intention (Sommestad et al., 2019). However, in our study, perceived behavioral control does not have a significant effect on information security protective behavioral intention. A possible explanation for this result is that the information security domain is challenging and multifaceted. Hence, perception of the ease or difficulty of tasks alone cannot lead to protection motivation. People's perception of this factor tends to vary, with each individual having a unique perception of the ease of work performance.

5. Discussion

This work contributes significantly to the information security field by identifying potential determinants of information security behavioral intention for IS researchers and practitioners from a broader perspective. By using work-related organizational constructs, protection motivation theory, and theory of planned behavior, this work has made significant contributions to IS theory-building by (a) incorporating organizational commitment and job satisfaction as key organization-related constructs of behavioral science theories-based models; (b) testing fear as a potential mediator in the model; and (c) adding three constituents, subjective norms, attitude, and perceived behavioral control, to enrich the understanding of protection intentions and behaviors in organizations. The findings of this study along with their implications elicit further discussion and offer new directions for further research.

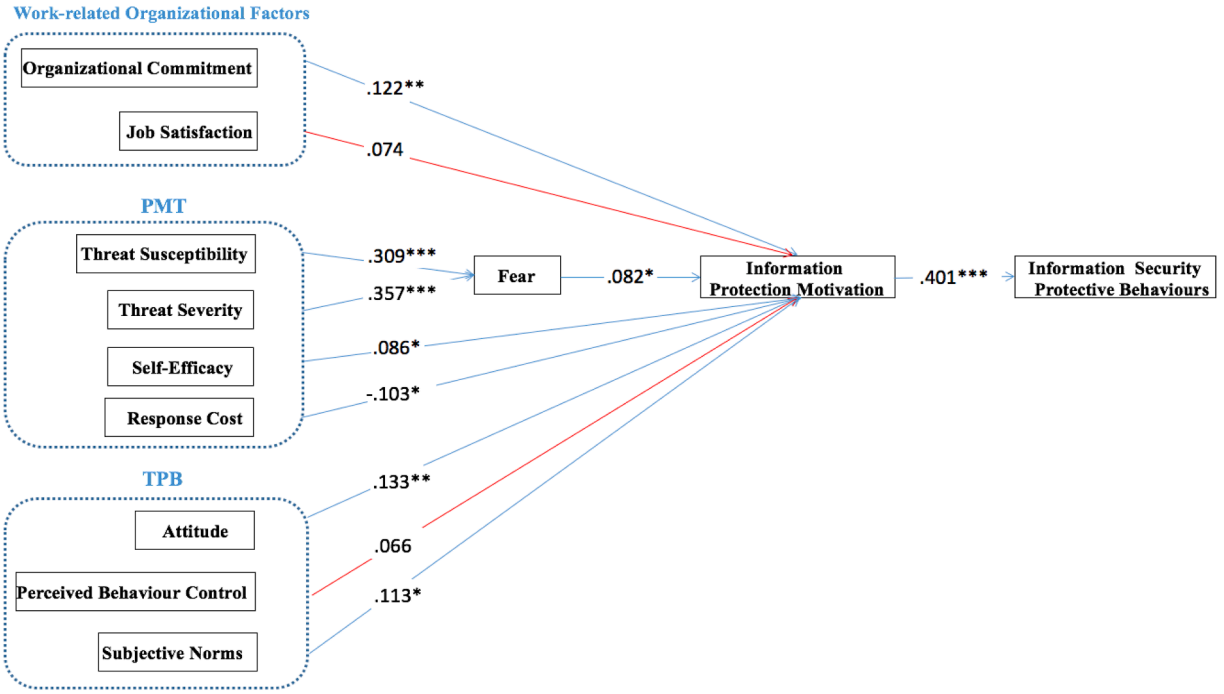

Fig 2. Research Results.

First, the above specified research detects that the work-related organizational variable, organizational commitment, strongly explains information security protective intention and positively impacts actual protective behaviors. The path between organizational commitment and protective information security behavioral intention indicates that IS professionals tend to have higher psychological investment in the organization and thus higher commitment to putting extra time and effort into protecting information assets. Surprisingly, H2, the association between job satisfaction and information assets protection motivation, was not supported by results, implying that job satisfaction is not a predictive antecedent to protection motivation for IS professionals. This conclusion, we have confidence in emphasizing that people with low work satisfaction are more concerned with individual advantages than with organizational information assets. This is important for data security tasks in today's environment as alluded through the lively nature of modern Chinese technology organizations. In such organizations, the reported actual rate of labor movement is higher than in most mature economies at 16% and becomes a substantial development issue (Gong et al., 2011; Xiao & Cooke, 2012). Although this study did not test the effects of job satisfaction on turnover intention directly, it reminds organization leaders to turn their attention to IS professionals' feelings, such as liking and enjoyment of the job (i.e., affective job satisfaction), to improve information security. Based on the above, our study exposes that the key to encouraging Chinese IS professionals' protective behaviors from work-related perspectives is to enhance their level of company commitment. This missing link in the information security chain in the Chinese context is a strong determinant of IS experts' protective behavioral intentions and actual behaviors. Building job satisfaction among IS employees with the objective of organizational security is a daunting challenge because it needs not only the satisfaction of employees' needs (e.g., work-life balance, bonus, and welfare), but also the building of 'a pleasant and harmonious organization climate' (Liu et al., 2020, p.11).

Second, for the PMT model, this study confirmed that fear increases intentions to involve in protective security actions as well as actual protective behaviors; this is in line with previous research that found that fear has a substantial impact on employees' security motivations, intentions, and behaviors (Boss et al., 2015; Johnston et al., 2015). This study further discovered that perceived threat susceptibility and perceived threat severity associated with information threats were significant predictors of fear. That said, IS experts who experience a strong sense of fear as a result of threat appraisal will have stronger behavioral intentions and more numerous actual protective behaviors. For example, targeted security education and training programs should reinforce the importance of protecting information security and specify the employees' responsibility to do so (Puhakainen & Siponen, 2010). Previous research supports this, finding that whenever organization managers disseminate fear, their information security subordinates reify their identities as protectors of organizational information security (Wall & Buche, 2017). IS professionals may hide the fear affected by information security threat susceptibility and threat severity or take it for granted, while ensuring they respond to specific protective responsibilities.

Third, this study found that the appraisal of coping mechanisms (i.e., response cost and self-efficacy) has significant effects on protective behavior intentions. Similar studies (Herath & Rao, 2009; Herath et al., 2014; Siponen et al., 2010) have assessed the effects of response cost and self-efficacy on IS policy compliance intention as well as users' behavioral intentions to use email authentication systems. For example, Herath et al. (2014) demonstrated that email screening response cost had a significant negative influence on attitude toward perceived usefulness of email authentication because of the tedious process involved with using email security

technologies. The outcoming of a cognitive cost-beneficial scrutiny is the perception of response cost which is given, Chinese IS professionals have a positive perception of the cost-benefit of implementing recommended protective behaviors, sacrificing time and effort, and incurring other costs to protect their organization's information. Hence, they invest more in building stronger security defence systems to counter information threats. Importantly, self-efficacy is also confirmed as one of the coping appraisals that make IS experts more likely to conduct protective information security behaviors if they have the relevant skills, confidence, competence, and capability to take information security precautions and implement preventative security measures. In sum, the results show that response cost and self-efficacy, the mechanisms of coping appraisal, have strong effects on information security protection motivation. They support the prediction that IS employees' relevant protective behaviors are enhanced when they believe that coping confidence is high and that the cost of performing the duty that protects information assets is worth paying.

Fourth, the results of data analysis show that work-driven information security protective behavior intentions can be explained by theoretical variables drawn from the theory of planned behavior. Two measurements, attitude and subjective norms, were found to have significant positive associations with work-driven information security behaviors, while perceived behavioral control did not. These results imply that an IS professional's attitude toward protective behaviors around threats (e.g., data breach issues) and the impact of significant others, such as managers and colleagues, play pivotal roles in facilitating information security protective behaviors, which aligns with the findings of relevant previous studies (Haeussinger & Kranz, 2013; Safa et al., 2015). As defined above, subjective norms in organizations refer to individuals' perceptions of what significant others think about duty-bound information security behaviors. One plausible explanation for this finding is that information security protective behavior intention can be affected by the opinions and perceptions of peers and other influential people in an individual's immediate environment. Thus, management can ensure the success of information protection programs by identifying and tasking influential people within the organization capable of motivating or shaping the opinions of others to 'champion the cause of the ISSP (Information Systems Security Policy) compliance in their contexts' (Ifinedo, 2014, p. 91).

5.1. Contributions to research

The theoretical contributions of this study can be understood in three ways. First, the interesting PMT results, which, unlike prior PMT research, included fear, emphasize that fear is a core assumption of proper PMT use. The model shows that the greater the fear, the stronger the protective motivation, especially when it influences actual behaviors. If threat appraisal messages do not result in the perception of fear, IS professionals will be less likely to perceive the importance of their roles in protecting information security from threats. The widespread lack of use of fear may be a problematic omission in information security research. Ignoring the implications of fear may lead to potentially spurious and misleading results that undermine the structured PMT nomology.

Second, extant information security studies have focused on security-related intention rather than actual behavioral change. According to Floyd et al. (2000) and Boss et al. (2015), PMT, although an intentions-focused model, has been effectively extended to actual behaviors. In this study, measurement of both intentions and actual behaviors has demonstrated the importance of actual information security protective behaviors in achieving the goal of improving these behaviors as well as stimulating protective intentions.

Third, this study advances theoretical implications by lending credence to the roles of two behavioral science theories, PMT and TPB, in establishing protective information security behaviors in Chinese IT organizations. Because information security protective behaviors are rational actions, this study constructs a comprehensive theoretical framework that includes protection-motivated variables (i.e., threat susceptibility, threat severity, response cost, and self-efficacy) and planned behavior factors (i.e., attitude, perceived behavioral control, and subjective norms) to help us understand the process by which actual protection-related behaviors are formed. The results of the data analysis support our major hypotheses, indicating that the two theories provide a good explanation for responsible behavior. The introduction of these theories not only provides new theoretical perspectives for understanding this specific behavior but also extends their application scope by verifying their explanatory power in the current research domain. Consistent with the theories' postulates, our findings pinpoint the fact that IS experts' behavioral intentions are circumscribed by social imperatives, attitudes, and threat and coping appraisals.

Fourth, while the role of organizational commitment in the information security area has been explored and explained by researchers and practitioners (Posey et al., 2015), its effect on Chinese IT organizations has not. This research demonstrates that organizational commitment is a key construct in motivating IS professionals' performance of protecting information security within organizations and suggests that its direct effect on information protection motivation is to serve as a catalyst in the chain of information security, making high-commitment IS professionals more proactive in countering potential threats. The addition of organizational commitment allows the current theoretical model to offer a new and deeper understanding of IS professionals' protection motivation.

5.2. Implications for practice

This study provides substantive practical implications for IT organizations struggling to enhance IS professionals' protective behaviors.

First, given the importance of attitude and subjective norms in determining protective behaviors, leaders of organizations should set up the belief that a close relationship with subordinates plays a vital role in ensuring organizational information security. Team managers should communicate actively with IS professionals, listening to their opinions, considering their suggestions, understanding and helping them tackle their difficulties, and providing more opportunities for career development (Liu et al., 2020). The more leaders enhance higher-quality communication with IS professionals, the more likely they are to build a feeling of obligation to repay the organization by protecting the security of information assets.

Second, this research reveals the critical nature of organizational commitment as a strong motivator of IS employees' protective behaviors. Organizations should increase efforts to strengthen the experts' feelings of identification and belongingness. Since high-commitment IS employees have a strong internal energizing force to protect information assets, organizations can motivate them further to share their experience and skills with other ordinary employees so that they perform protective behaviors together. This approach can improve employees' perception and cognition of their importance to the organization and its membership.

Third, the effectiveness of threat and coping appraisals in Chinese IT organizations means that information security issues could lead to negative social influence. Hence, training that includes sharing relevant cases of severe information security threats is highly recommended. During training, organizations should constantly highlight the importance of information security protection and emphasize the severe consequences of non-protective behaviors. At the same time, they should constantly promote the development of skills needed to improve safeguarding actions.

6. Limitations and directions for future studies

The current research presents some limitations that open up new opportunities for future studies. First, some IT professionals might have offered socially desirable responses to certain questions in an attempt to maintain their organization's reputation (Podsakoff et al., 2003). Therefore, the answers might have been skewed to negatively impact the data analysis. Further, the data was based on a cross-sectional survey, while longitudinal data may have facilitated more insight. Future studies could use qualitative research methods such as in-depth interviews and focus groups to investigate actual information security protective behaviors and enrich insights.

Second, this research focused on IS professionals in Chinese IT organizations. If the results were influenced by the cultural values of the organizations involved, their generalizability may have been compromised. Third, this study focused on IS employees' perceptions of information security protective behaviors. To increase knowledge in this domain, future research could examine the opinions of employees not working in information security, for example, outsourced staff (as outsourcing is a popular trend today). This would enable comparative analysis to test individuals' behavioral performance in the workplace with different levels of information security control, thus deepening the understanding of the subject matter.

7. Conclusion

To further illuminate the determinants of work-driven information security behaviors performed by IS professionals to cope with internal information security threats, we have shown the significance of elements associated with protection motivation theory and theory of planned behavior. This paper presents novel research that shows how work-driven information security protective behaviors are formed based on information security attitudes, subjective norms, threat susceptibility, and threat severity. We also detail the roles of often neglected factors such as organizational commitment and job satisfaction in the mitigation of information security threats. Moreover, the efforts were shown to bolster components in coping appraisal, such as self-efficacy and response costs. These two are more likely to impact individuals' protection motivation and protective behaviors toward tackling potential information security issues. This research endeavor has enhanced our understanding of Chinese IS professionals' behavioral performance.

Author Statement

Ma Xiaofen is a doctoral candidate in Department of Communications and New Media at the National University of Singapore. Her research interests are in social media users' online privacy management and information security protection in IT organizations.

Declaration of Competing Interest

We acknowledge that no conflict of interest exits in the submission of this manuscript, and manuscript is approved by author for publication. All authors that the work described was original research that has not been published previously, and not under consideration for publication elsewhere, in whole or in part. All the authors listed have approved the manuscript that is enclosed.

References

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior1. *Journal of Applied Social Psychology, 32*(4), 665–683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x.

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security, 28*(6), 476–490. https://doi.org/10.1016/j.cose.2009.01.003.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643. https://doi.org/10.2307/25750694.

Block, L. G., & Keller, P. A. (1995). When to accentuate the negative: The effects of perceived efficacy and message framing on intentions to perform a health-related behavior. *Journal of marketing research, 32*(2), 192–203. https://doi.org/10.1177/002224379503200206.

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 security 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 policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690.

CAC (2019).互联网百强企业去年收入达2.75万亿-中共中央网络安全和信息化员 会办公室. Retrieved from http://www.cac.gov.cn/2019-08/15/c_1124879465.htm.

Cammann, C. (1983). Assessing the attitudes and perceptions of organizational members. Assessing organizational change: A guide to methods, measures, and practices, 71-138.
Chang, A. J., Wu, C., & Liu, H. (2012). The effects of job satisfaction and organization commitment on information security policy adoption and compliance. In *Proceedings of the IEEE international conference on management of innovation & technology (ICMIT)* (pp. 442–446). IEEE. https://doi.org/10.1109/ICMIT.2012.6225846.
Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (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, 1016/j.cose.2013.09.009.
Cox, J. (2012). Information systems user security: a structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003.
Cronbach, L. J., & Shavelson, R. J. (2004). My current thoughts on coefficient alpha and successor procedures. *Educational and Psychological Measurement, 64*(3), 391–418. https://doi.org/10.1177/0013164404266386.
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.
Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviours: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database, 45*(4), 51–71. https://doi.org/10.1145/2691517.2691521. The Database for Advances in Information Systems.
Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. *Management Science, 31*(2), 134–149. https://doi.org/10.1287/mnsc.31.2.134.
Eppright, D. R., Hunt, J. B., Tanner, J. F., & Franke, G. R. (2002). Fear, coping, and information: A pilot study on motivating a healthy response. *Health Marketing Quarterly, 20*(1), 51–73. https://doi.org/10.1300/J026v20n01_05.
Fatimah, O., Amiraa, A. M., & Halim, F. W. (2011). The relationships between organizational justice, organizational citizenship behaviour and job satisfaction. *Pakistan Journal of Commerce and Social Sciences, 19*(5), 115–121. Retrieved from http://web.b.ebscohost.com.libproxy1.nus.edu.sg/ehost/pdfviewer/pdfviewer?vid=2&sid=1b10f4bb-b58d-43b8-b17f-59e349a1a3dc%40pdc-v-sessmgr02.
Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x.
Fishbein, M., & Ajzen, I. (1981). On construct validity: A critique of Miniard and Cohen's paper. *Journal of Experimental Social Psychology, 17*(3), 340–350. https://doi.org/10.1016/0022-1031(81)90032-9.
Gong, Y., Gong, Y., Chow, I. H., Chow, I. H., Ahlstrom, D., & Ahlstrom, D. (2011). Cultural diversity in China: Dialect, job embeddedness, and turnover. *Asia Pacific Journal of Management, 28*(2), 221–238. https://doi.org/10.1007/s10490-010-9232-6.
Greene, G., & D'Arcy, J (2010). Assessing the impact of security culture and the employee-organization relationship on IS security compliance. In *Proceedings of the 5th annual symposium on information assurance* (pp. 1–8). Retrieved from https://www.albany.edu/wwwres/conf/iasymposium/proceedings/2010/ASIA10Proceedings.pdf#page=51.
Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behaviour. In *Proceedings of the thirty fourth international conferences on information systems, Milan 2013* (pp. 1–16). Retrieved from, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.669.8230&rep=rep1&type=pdf.
Hassandoust, F., & Techatassanasoontorn, A.A. (2018). Understanding users' information security awareness and intentions: A full nomology of protection motivation theory. In Cyber influence and cognitive threats, 129-143. PACIS 2018 Proceedings. 93. Retrieved from https://aisel.aisnet.org/pacis2018/93.
Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005.
Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1), 61–84. https://doi.org/10.1111/j.1365-2575.2012.00420.x.
Herscovitch, L., & Meyer, J. P. (2002). Commitment to organizational change: Extension of a three-component model. *Journal of Applied Psychology, 87*(3), 474–487. https://doi.org/10.1037/0021-9010.87.3.474.
Holbert, R. L., & Stephenson, M. T. (2003). The importance of indirect effects in media effects research: Testing for mediation in structural equation modeling. *Journal of Broadcasting & Electronic Media, 47*, 556–572. https://doi.org/10.1207/s15506878jobem4704_5.
Hsu, M., & Kuo, F. (2003). An investigation of volitional control in information ethics. *Behaviour & Information Technology, 22*(1), 53–62. https://doi.org/10.1080/01449290301781.
Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118.
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 socialisation, influence, and cognition. *Information & Management, 51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001.
Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005.
Johnson, R. D., & Marakas, G. M. (2000). The role of behavioral modeling in computer skills acquisition: Toward refinement of the model. *Information Systems Research, 11*(4), 402–417. https://doi.org/10.1287/isre.11.4.402.11869.
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566. https://doi.org/10.2307/25750691.
Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06.
Kim, J. H., & Mun, H. J. (2018). Influences of affectivity and organizational commitment on job satisfaction and work performance of information security professionals. *Journal of the Korea Convergence Society, 9*(6), 225–234. https://doi.org/10.15207/JKCS.2018.9.6.225.
Lebek, B., Uffen, J., Breitner, M.H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. In Proceedings of the 46th hawaii international conference on system sciences (pp. 2978-2987). IEEE. 10.1109/HICSS.2013.192.
Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11.
Li, S., Tryfonas, T., & Li, H. (2016). The internet of things: A security point of view. *Internet Research, 26*(2), 337–359. https://doi.org/10.1108/IntR-07-2014-0173.
Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate Guanxi and organizational commitment. *International Journal of Information Management, 54*, Article 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152.
Lize, G., Jingpei, W., & Bin, S. (2014). Trust management mechanism for internet of things. *China Communications, 11*(2), 148–156. https://doi.org/10.1109/CC.2014.6821746.
Lu, Z. (2017). 倒卖信息可入罪 新法为个人信息穿上铠甲-新华网 [New law to put armor on personal information - xinhuanet.com].Retrieved from http://www.xinhuanet.com//politics/2017-06/14/c_1121138988.htm.
Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9.
Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security, 75*, 147–166. https://doi.org/10.1016/j.cose.2018.01.020.
Meyer, J. P., & Allen, N. J. (1997). *Commitment in the workplace: Theory, research, and application*. Sage.
Meyer, J. P., Allen, N. J., & Smith, C. A. (1993). Commitment to organizations and occupations: Extension and test of a three-component conceptualization. *Journal of Applied Psychology, 78*(4), 538–551. https://doi.org/10.1037/0021-9010.78.4.538.

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.
Mowday, R. T., Porter, L. W., & Steers, R. M. (2013). *Employee—organization linkages: The psychology of commitment, absenteeism, and turnover*. Academic press.
Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. In *Predicting health behaviour, 81* pp. 98–143). Mcgraw. Hill Education. Retrieved from https://new.iums.ac.ir/files/hshe-soh/files/predicting_Health_beh_avior(1).pdf#page=98.
Oplatka, I. (2009). Organizational citizenship behavior in teaching: The consequences for teachers, pupils, and the school. *International Journal of Educational Management, 23*(5), 375–389. https://doi.org/10.1108/09513540910970476.
Orazi, D. C., & Pizzetti, M. (2015). Revisiting fear appeals: A structural re-inquiry of the protection motivation model. *International Journal of Research in Marketing, 32*(2), 223–225. https://doi.org/10.1016/j.ijresmar.2015.02.003.
Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing, 67*(2), 1–18. https://doi.org/10.1509/jmkg.67.2.1.18607.
Peterson, R. A. (1994). A meta-analysis of Cronbach's coefficient alpha. *The Journal of Consumer Research, 21*(2), 381–391. https://doi.org/10.1086/209405.
Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879. https://doi.org/10.1037/0021-9010.88.5.879.
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.
Pratt, C., Fruin, D. J., & Owen, N. (1992). Protection motivation theory and adolescents' perceptions of exercise. *Journal of Applied Social Psychology, 22*(1), 55. https://doi.org/10.1111/j.1559-1816.1992.tb01521.x.
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.
Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93. https://doi.org/10.1080/00223980.1975.9915803.
Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153–176, 10004535663.
Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112–133. https://doi.org/10.1016/j.istr.2010.11.002.
Safa, N. S., & Ismail, M. A. (2013). A customer loyalty formation model in electronic commerce. *Economic Modelling, 35*, 559–564. https://doi.org/10.1016/j.econmod.2013.08.011.
Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012.
Safa, N. S., & Von Solms, R (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037.
Shepherd, L., Archibald, J., & Ferguson, R. (2014). Reducing risky security behaviours: Utilising affective feedback to educate users. *Future Internet, 6*(4), 760–772. https://doi.org/10.3390/fi6040760.
Spector, P. E. (1985). Measurement of human service staff satisfaction: Development of the job satisfaction survey. *American Journal of Community Psychology, 13*(6), 693–713. https://doi.org/10.1007/BF00929796.
Siponen, M., Adam, M. M., & 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.
Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer (Long Beach, Calif.),, 43*(2), 64–71. https://doi.org/10.1109/MC.2010.35.
Siponen, M. T., & Vance, A. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing, 24*(1), 21–41. https://doi.org/10.4018/joeuc.2012010102.
Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045.
Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. *The Journal of Computer Information Systems, 59*(4), 344–353. https://doi.org/10.1080/08874417.2017.1368421.
Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2015). Behavioral information security. *Human-Computer Interaction and Management Information Systems: Foundations*, 262–280.
Stanton, J.M., Stam, K.R., Guzman, I., & Caledra, C. (2003). Examining the linkage between organizational commitment and information security. Proceedings of the IEEE international conference theme-system security and assurance, 3, 2501-2506. doi:10.1109/ICSMC.2003.1244259.
Vance, A., Siponen, M., & Pahnila, S. (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.
Verkijika, S. F. (2018). Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security, 77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008.
Wall, J. D., & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems, 41*(1), 13. https://doi.org/10.17705/1CAIS.04113.
Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1*(4), 317–342. https://doi.org/10.1080/108107396127988.
Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *Proceedings of the association for information systems - 26th international conference on information systems, ICIS 2005*. Retrieved from, http://130.18.86.27/faculty/warkentin/securitypapers/Merrill/WoonTanLow2005_ICIS ProtectionMotivation.pdf.
Workman, M., Bommer, W. H., & Straub, D. (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. https://doi.org/10.1016/j.chb.2008.04.005.
Wu, D. (2020). Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behaviour. *Computers in Human Behaviour, 105*, Article 106229. https://doi.org/10.1016/j.chb.2019.106229.
Wu, J., & Wang, S. (2005). What drives mobile commerce? An empirical evaluation of the revised technology acceptance model. *Information & Management, 42*(5), 719–729. https://doi.org/10.1016/j.im.2004.07.001.
Xiao, Y., & Cooke, F. L. (2012). Work–life balance in China? Social policy, employer strategy and individual coping mechanisms. *Asia Pacific Journal of Human Resources, 50*(1), 6–22. https://doi.org/10.1111/j.1744-7941.2011.00005.x.
Yoon, C., & Kim, H. (2013). Understanding computer security behavioural intention in the workplace: An empirical study of Korean firms. *Information Technology & People, 26*(4), 401–419. https://doi.org/10.1108/ITP-12-2012-0147 (West Linn, Or.).
Zhang, X. J., Li, Z., & Deng, H. (2017). Information security behaviours of smartphone users in China: An empirical analysis. *Electronic Library, 35*(6), 1177–1190. https://doi.org/10.1108/EL-09-2016-0183.