Motivating Accounting Information Systems Security Policy Compliance: Insight from the Protection Motivation Theory and the Theory of Reasoned Action

Trung Nguyen Quoc(✉), Quyen Phan Thi Bao, Binh Nguyen Huu, and An Nguyen Phuoc Bao

University of Economics HCM City, Ho Chi Minh City, Vietnam
nguyenquoctrung@ueh.edu.vn

Abstract. This study aims to explore the factors that motivate individuals to comply with accounting information systems security policies (AISSP) in Vietnam based on the Protection Motivation Theory (PMT) and the Theory of Reasoned Action (TRA). The survey method was acquired for doing the study. Our findings were interpreted based on the data collected from 226 accountants in Vietnam through a self-administrated questionnaire. The psychometric properties of the theoretical model and proposed hypotheses were assessed by the PLS-SEM technique on SmartPLS 3.2.7. The results show that the PMT and TRA model performs well in Vietnam, with a 58.1% variance in behavior to comply with the AISSP explained by the model. Direct/ indirect positive impacts on AISSP compliance behavior may have resulted from the coping appraisal, attitude to comply with AISSP, and subjective norms. This study recommends that management can boost employees' AISSP compliance behavior by instituting regular IS security awareness sessions, campaigns, and training. In addition, management might encourage employees to acquire the skills and knowledge required to secure the IS assets of the firm. The findings from this study contribute to a better understanding of the mechanism of establishing and enhancing the employees' AISSP compliance behavior in particular, as well as ISSP compliance behavior in general in organizations.

Keywords: Threat Appraisal · Coping Appraisal · Attitude · Subjective Norms · Intention · And Compliance Behavior

1 Introduction

In the modern corporate world, firms face numerous dangers to their information systems. If organizations and system users are not entirely aware of dangers and their systems are not adequately safeguarded, system security risks will increase; especially when the Internet and improvements in information technology increasingly support the operation of the information system.

P. Tra Lam and P. Quang Huy (Eds.): ICECH 2022, AEBMR 238, pp. 342–359, 2023.
https://doi.org/10.2991/978-94-6463-150-0_23

In response to these issues, information system security policies are published to guide and steer the behavior of system users in order to achieve the information system security objectives. Problematically, system users (i.e., employees, managers, etc.) do not always comply freely with the ISSP. Therefore, chief security officers are primarily concerned with enforcing information system security policies. Furthermore, they must determine how to ensure that staff adheres to ISSP.

To address this limitation, an increasing number of academics are focusing on security policy issues and policy compliance behavior of system users (Alias, 2019). In particular, the analyzing factors influencing compliance/noncompliance with the ISSP has been a high priority for academics in this discipline. Numerous theories from other domains have been applied to information system security research in order to identify and explain the factors that influence information systems security policy compliance behavior (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014). Protection motivation theory is one of the most commonly applied behavioral theories (Boss, Galletta, Lowry, Moody, & Polak, 2015)) to explain the influence of motivational factors on individuals' compliance behavior in a variety of contexts; highlighting the significance of improving employee motivation and examining the influence of external and internal motivating factors on compliance behavior (Herath & Rao, 2009a). However, research practice indicates that prior studies have not utilized all parts of the protection motivation theory concurrently to explain employee compliance intents and behaviors (Ali, Dominic, Ali, Rehman, & Sohail, 2021). This drives us to conduct a study addressing the need for ISSP compliance behavior research on protective motivation. Specifically, protective motive theory and the theory of reasoned action are combined to explain the process of influence of two factors, namely threat appraisal and coping appraisal, on the employee's ISSP compliance behavior.

With the increasing trend toward accounting-related technology applications, the organization becomes more heavily dependent on accounting information systems (AIS); hence, the AIS power is more substantial (Ezzamel & Bourn, 1990). Nevertheless, increased AIS power brings its increased vulnerability (Ezzamel & Bourn, 1990), especially in today's digital era. ISSP (including accounting information systems security policy AISSP) is expected to provide precise regulations and guidelines to protect the AIS assets of an organization from intentional abuse or destruction (adapted from Son (2011)). Therefore, it is necessary to understand better the factors that promote AISSP compliance behavior. This research adds to the existing body of knowledge in several ways. First, our study sheds light on how threat appraisal, coping appraisal, attitude to comply, and subjective norms influence actual AISSP compliance behavior via the mediation of intent to comply. Second, our study provides data and empirical evidence from an economy in transition, Vietnam, where technology solutions are altering the design and operation of commercial information systems, but the security issue of these systems has not been given sufficient consideration.

The remaining pieces of paper are organized as shown. In the following section, we give the literature review, followed by the theoretical backdrop and elaboration of hypotheses. Following this part is a discussion of the data collection methods, sampling strategy, and data analysis. Finally, the results and discussion are presented, followed by the theoretical and managerial implications, as well as the study's limitations.

2 Theoretical Background and Statements of Hypotheses

2.1 Theoretical Background

In research on Information Systems Security Policy (ISSP), theories of behavioral science such as Protection Motivation Theory (PMT), Technology Acceptance Model, Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), and General Deterrence Theory (GDT) are prevalent and frequently employed (Lebek, Uffen, Neumann, Hohler, & H. Breitner, 2014). Depending on the unique research situation, each theory may be utilized alone or in conjunction with other theories to explain variables influencing ISSP compliance behaviors.

Son (2011) explains that ISSP compliance behavior is the act of complying with the standards for employee responsibilities and obligations, the management of organizational security, as well as knowing the punishments and the act of coping with non-compliance. ISSP compliance behavior is also exhibited by assessing the extent to which employees encourage and support the compliance of other individuals within the business (Siponen, Pahnila, & Mahmood, 2014).

Studies on ISSP compliance behaviors frequently use a combination of theories to explain the effects of antecedents on individual compliance behaviors, such as: PMT, TRA, and GDT (Pahnila, Siponen, & Mahmood, 2007b); PMT and Social cognitive theory (Workman, Bommer, & Straub, 2008), PMT and GDT (Herath & Rao, 2009b); PMT and fear appeals model (Johnston & Warkentin, 2010); PMT, GDT, TRA, and innovation diffusion theory (Siponen et al., 2010); PMT and TPB (Ifinedo, 2012); PMT and habit theory (Vance, Siponen, & Pahnila, 2012); PMT, TRA, and Cognitive Evaluation Theory (Siponen, Mahmood, & Pahnila, 2014); PMT and GDT (Warkentin, Siponen, & Johnston, 2015). Similarly, this study uses a combination of PMT (Rogers, 1975) and TRA (Fishbein & Ajzen, 1977) with aims to explain and establish the influence mechanism of threat appraisal and Coping appraisal on ISSP compliance behaviors.

Protection Motivation Theory (PMT), which developed by Rogers (1983) expanded the health-related belief model in the social psychology and health domains (Milne, Sheeran, & Orbell, 2000; Rippetoe & Rogers, 1987). PMT was created to aid in the clarification of fear appeals, and it draws from the expectancy-value and cognitive processing theories. PMT has been called one of the most powerful explanatory theories to forecast whether an individual would take preventative measures (Anderson & Agarwal, 2010). This theory discusses how both internal and external motivators affect compliance behavior in different settings, highlighting the significance of fostering a more motivated workforce (Herath & Rao, 2009c). To sum up, both the threat appraisal and the coping appraisal are the sources of protection motivation. An individual's evaluation of the severity of a threat is known as a "threat appraisal" (Ifinedo, 2012; Rogers, 1983; Woon, Tan, & Low, 2005). It consists of the two parts listed below:

- Vulnerability refers to the likelihood of a negative event occurring if precautions are not taken. In this analysis, vulnerability refers to a company's estimation of how susceptible it is to IS security threats in the absence of preventative measures, such as adhering to AISSP guidelines (Vance et al., 2012)

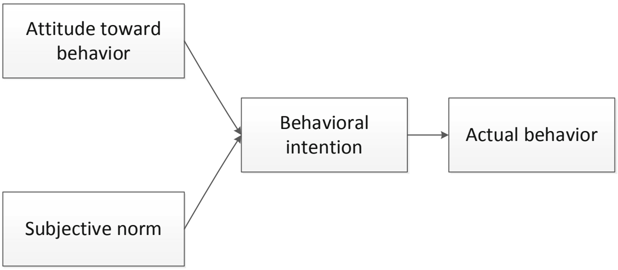

Fig. 1. Theory of Reasoned Action (Adapted from Davis et al. (1989))

- Severity is the level of the potential impact of the threat (i.e., its severity and how severe the damage that it can cause). In this context, it denotes the seriousness of the AIS security breach and the potential damage that could result from the breach to the enterprise (Vance et al., 2012)

According to Woon et al. (2005), coping appraisal refers to an individual's ability to cope and prevent potential loss or damage arising from a threatening event, including:

- Self-efficacy – This concept emphasizes an individual's ability or judgment to cope or perform recommended behavior. Specifically, in the context of this research, self-efficacy is an employee's belief that they can successfully implement and comply with the AISSP (Vance et al., 2012)
- Response efficacy – this concept is related to beliefs about the benefits obtained from the actions taken by the individual) (Rogers, 1983). For the scope of this article, response effectiveness is the belief of employees that compliance with the AISSP will be effective in reducing a safety threat (Vance et al., 2012)
- Response cost focuses on how much time, money, and effort people believe they will have to put into implementing the suggested action. Accordingly, response cost could be the opportunity cost of complying with AISSP. In light of the fact that the research informants are accounting-function-related employees, they do not have sufficient information about actual expenses related to information systems security policy; this factor thus will be removed from the concept of coping appraisals.

The Theory of Reasoned Action (TRA) is found in social psychology literature. TRA enhances the expectancy-value theory's ability to forecast and provide an explanation. The TRA elucidates the causes of deliberate action (Ajzen & Fishbein, 1975; Fishbein & Ajzen, 1980) that a person's performance of a specific behavior is determined by his or her behavior intention to perform the behavior (Davis, Bagozzi, & Warshaw, 1989). Eveland (1986) observes that "ultimately, technology transfer is a function of what individuals think – because what they do depends on those thoughts, feelings and interests" (p.310).

TRA, shown in Fig. 1, posits that the person's attitude and subjective norms concerning intention to comply ISSP (Davis et al., 1989), which in turn leads to actual behavior.

2.2 Threat Appraisal

The previous research results show threat appraisal positively influences the intention to comply with ISSP through the mediating role of attitude towards ISSP compliance. (Pahnila, Siponen, & Mahmood, 2007a). Warkentin et al. (2015) based on PMT showed that Enhanced fear appeal (threat appraisal and coping Appraisal) has a material impact on intention towards ISSP compliance and ISSP compliance behaviors. Besides, PMT constructs (threat appraisal, self-efficacy) visibility positively affect the intention to comply with ISSP as well as deterrence and intention are the best predictors of actual compliance behavior towards ISSP (Siponen et al., 2010). Perceived vulnerability also positively influences employees' ISSP behavioral compliance intentions (Ifinedo, 2012). On these bases, the following research hypotheses are proposed:

H_{1a}: Threat appraisal of accounting information system security has a direct, positive and significant impact on AISSP compliance behaviors.

H_{1b}: Threat appraisal of accounting information system security has an indirect, positive and significant impact on AISSP compliance behaviors through intention to comply with AISSP.

2.3 Coping Appraisal

According to (Pahnila et al. (2007b), coping appraisal positively affects the intention to comply with ISSP through mediating role of attitude towards ISSP compliance (Pahnila et al., 2007a). In addition, the research results of Johnston and Warkentin (2010) indicate that response effectiveness, self-efficacy have a positive impact on employees' behavioral intention in using antispyware software tools. Siponen et al. (2010b) assert that PMT constructs, including coping appraisal, also positively affect the intention to comply with ISSP. In the experimental research model, Ifinedo (2012) also concludes that self-efficacy, response efficacy, and attitude toward compliance also positively influence ISSP behavioral compliance intentions of employees. Primarily based on PMT, Blythe and Coventry (2018) indicate that coping appraisal was more predictive than threat appraisal to detect employees' intention to engage in antimalware behaviors. Most recently, according to research by T Alanazi, Anbar, A Ebad, Karuppayah, and Al-Ani (2020), self-efficacy is the most influential factor in information security compliance behavior.

On these bases, the following research hypotheses are proposed:

H_{2a}: Coping appraisal of accounting information system security has a direct, positive and significant impact on AISSP compliance behaviors.

H_{2b}: Coping appraisal of accounting information system security has an indirect, positive and significant impact on AISSP compliance behaviors through intention to comply with AISSP.

2.4 Attitude to Comply with ISSP

Based on the proposal that conforming attitude will lead to conforming behavior of PMT, the relationship between attitude and behavioral intention has been extensively experimental studied in information system theory (Venkatesh, Morris, Davis, & Davis, 2003). Besides that, TRA of Ajzen (1991) shows that an individual's attitude affects behavioral intention. This means a positive attitude will increase an individual's intention to comply with ISSP, and vice versa. As a result, individuals with positive beliefs and values about the organization's ISSP will be more inclined to comply with the rules, requirements, and guidelines of that security policy. (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009b). On the contrary, individuals who lack a positive attitude are unwilling to comply with the policy (Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009; Pahnila et al., 2007b). In the context of ISSP compliance behaviors, many research results using TRA also show that attitude positively affects individuals' intention to comply. (Bulgurcu et al., 2010; Ifinedo 2012, 2014; Pahnila et al., 2007a; Safa et al., 2015; Safa, Von Solms, & Furnell, 2016). In this study, the attitude to comply with ISSP addresses the importance, benefits and usefulness of adopting security technology and security practices (Fishbein & Ajzen, 1977).

Experimental studies on the mechanism of action of attitude to comply with ISSP achieved the following results: Ifinedo (2012) affirms that attitude toward compliance positively influences ISSP behavioral compliance intentions of employees. In the study by Yoon and Kim (2013), the research results show that the attitude towards computer security significantly affects employees' behavioral intentions. In the same year, indicates that attitude, perceived behavioral control, organizational commitment, and subjective norms have significant effects on behavioral intent. Continuing this research trend, Bélanger, Collignon, Enget, and Negangard (2017) publish attitude and intention are significant predictors of actual early compliance behavior towards information security policy.

On these bases, the following research hypotheses are proposed:

H_{3a}: Attitude to comply with AISSP has a direct, positive and significant impact on AISSP compliance behaviors.

H_{3b}: Attitude to comply with AISSP has an indirect, positive and significant impact on AISSP compliance behaviors through intention to comply with AISSP.

2.5 Subjective Norms

Subjective norms refer to the cues, ideas, and incentives to comply with a particular act that are determined mainly by seeking advice from or observing the actions of others (Ajzen, 1991). Researchers have discovered that people's actions are prompted or impacted by the social norms they see around them (Chan, Woon, & Kankanhalli, 2005; Johnston & Warkentin, 2010; Knapp, Marshall, Rainer, & Ford, 2006). For example, when it comes to ISSP compliance in the workplace, workers are more inclined to follow the rules if they see that their bosses, coworkers, and subordinates are doing the same (Chan et al., 2005). Organizational ISSP compliance is highly impacted by subjective norms, according to research by (Bulgurcu et al., 2010; Herath & Rao, 2009a, 2009b; Lee & Larsen, 2009; Pahnila et al., 2007b). Consequently, the following hypotheses are put forth:

H_{4a}: Subjective norms have a direct, positive and significant impact on AISSP compliance behaviors.

H_{4b}: Subjective norms have an indirect, positive and significant impact on AISSP compliance behaviors through intention to comply with AISSP.

2.6 Intention to Comply with AISSP

While PMT suggests that the intention to comply will lead to complying behavior, the model of TRA theory also asserts that a person's behavior is determined by this individual's behavioral intention to do it. This means TRA focuses on explaining the relationship between behavioral beliefs, individual attitudes, subjective norms, intentions, and behaviors. Accordingly, an individual's behavior is determined by the intention to perform that behavior. Intention to engage in a behavior is determined by their attitudes and subjective norms toward that behavior, in other words, if any person expects a positive outcome (attitudes) as well as there are essential others who are also inclined to desire the behavior (subjective norms: the rules, beliefs, and dynamics of society that guide individuals to follow a particular action) then that positive intention is likely to lead to this behavior Ajzen and Fishbein (1975).

The relationship between intention and behavior has been extensively experimental studied in the theory of PMT, GDT, TPB, TRA. Specifically, all studies on the impact of concepts belonging to PMT, GDT, TPB, TRA conclude that the intention to comply with ISSP impacts the behavior of complying with ISSP. (Bélanger et al., 2017; Blythe & Coventry, 2018; Siponen, Pahnila, & Mahmood, 2006; Siponen & Vance, 2010; Son, 2011). In this study, intention to comply with AISSP refers to an individual's intention to comply with the AISSP and assist others in the same organization to comply with the AISSP.

On these bases, the following research hypothesis are proposed:

H_5: Intention to comply with AISSP has a positive and significant impact on AISSP compliance behaviors.

In conclusion, a theoretical model was developed by summarizing and arguing related theories to show the relationship between six research concepts: (1) Threat appraisal of accounting information system security; (2) Coping appraisal of accounting information system security; (3) Attitude to comply with AISSP; (4) subjective norms; (5) Intention to comply with AISSP and (6) AISSP compliance behaviors. A total of nine research hypotheses have been formulated to demonstrate the direct and indirect effects of threat appraisals, coping appraisals, attitude and subjective norms on AISSP compliance behaviors (Fig. 2).

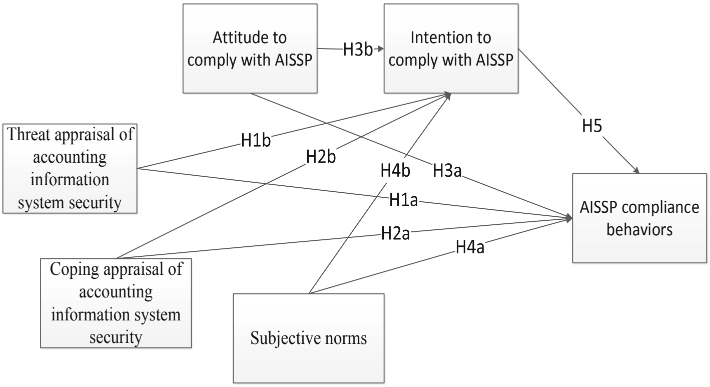
Attitude to comply with AISSP
H3b
Intention to comply with AISSP
H5
Threat appraisal of accounting information system security
H1b
H2b
H4b
H3a
H1a
H2a
H4a
AISSP compliance behaviors
Coping appraisal of accounting information system security
Subjective norms

Fig. 2. Proposed research model

3 Research Methodology

3.1 Data Collection and Participants

This research aims to collect information from Vietnam's medium and large businesses working in various disciplines and industries. Survey-collected primary data was utilized for the analysis. Potential participants were accounting-function-related employees who utilize computers and the Internet as part of their everyday work at the companies polled. Specifically, 50 potential respondents working in different job positions from each enterprise, out of a total of 30 potential businesses, were invited to participate in the online pilot survey. Ensuring the heterogeneity of the sample by considering different types of companies and collecting surveys from individuals with varied accounting-related responsibilities in the business aids in the generalizability of the research results. To guarantee that the firms surveyed are suitable for the aims of the study, we utilized three questions to establish that each enterprise has an ISSP. Specifically, respondents were asked: (1) Does the organization have its own IT department? (2) Does the business have a yearly budget for information system security? (3) How long has the ISSP been implemented at the organization? Moreover, to ensure that the employed questionnaire supplied participants with clear information about the study's idea, we provided a definition of ISSP (please see Appendix).

Before conducting the survey, we contacted each company's management to obtain permission to interview their employees and receive email lists of potential project participants. Based on this, a list of email addresses for data collection is produced. The online survey questionnaire was then emailed to 1,500 prospective employees at businesses whose email addresses were included in the list of addresses.

The data collection process is managed by SurveyMonkey software. After two weeks, reminder emails will be sent to responders who have not responded. After 1.5 months of collecting data and mailing emails four times, we obtained 451 responses. However, only 226 valid responses were received following the exclusion of invalid responses (e.g., incomplete responses, response time less than 5 min, working experience in the current position is too small, or not appropriate respondents). These valid answers indicate that the company has its own IT department. In addition, roughly 89% of respondents acknowledged that their companies had a separate annual budget for guaranteeing the security of their information systems; the remainder are unsure. In particular, more than 33% of respondents indicated that the ISSP has been implemented at their organization for more than 10 years, with the remainder having adopted it for at least 6 months. Respondents are qualified to speak on the topic of compliance with information system security policy because they are now employed by businesses that have been implementing information system security policies and hence have sufficient expertise and knowledge to do so. The following table describes in full the sample characteristics (Table 1).

Table 1. Sample characteristics.

	Frequency	Percentage
Gender		
Female	*122*	*54*
Male	*104*	*46*
Total	226	100.0
Age		
<25	*17*	*7.5*
25–34	*125*	*55.3*
35–44	*69*	*30.5*
>44	*15*	*6.7*
Total	226	100.0

3.2 Variable Measurement

All latent variables of interest were measured by instruments that had been previously developed and used in the literature. This contributes to enhancing the validity and reliability of our study (Straub, Limayem, & Karahanna-Evaristo, 1995). Threat appraisal was measured by two components: perceived severity, and vulnerability. In which perceived severity and vulnerability were measured using three items for each variable modified from (Siponen et al., 2010b). The coping appraisal in this study was also measured by two components: response efficacy, and self-efficacy. They were measured by using three statements employed for each variable from (Siponen et al., 2010b). Attitude to comply with AISSP was measured by a three-item scale developed for this study based on Fishbein and Ajzen (1977)'s instrument. Intention to comply with AISSP and AISSP compliance behaviors were measured by using three statements for each variable derived from (Siponen et al., 2010b). According to Herath and Rao (2009b), subjective norms construct is measured by five items. To sum up, there are eight latent variables in total. Respondents were asked to rate the extent to which they agree with the statements on a seven-point Likert scale, ranging from 1 "Strongly disagree" to 7 "Strongly agree".

To ensure that the content value of the scale is completely appropriate in the research context, in different way, the question reflects the content that needs to be asked, the scale would be evaluated by an expert group via email. This group consists of three academics in the fields of accounting information systems and accounting information security, and five experts with practical experience (two accounting professionals in the corporates and three workings in enterprise network security). These experts are encouraged to provide feedback on the completeness and relevance of the questionnaire. The experts reviewed the revised version of the questionnaire several times to reach a consensus on the clarity and relevance of the content of the question. A pilot test would then be carried out to estimate the time needed to complete the survey and ensure that the questions' content is clear, understandable, and free of duplication. A group of graduate students majoring in information systems and accounting staff from several organizations (minimum 10 people) was then chosen to perform the pilot. Finally, statement modifications would be considered and adjusted by the authors to develop the final questionnaire.

4 Analyses and Results

PLS-SEM analysis technique was utilized instead of CB-SEM. This method is appropriate for validating predictive model that incorporate higher-order constructs (Hair Jr, Sarstedt, Hopkins, & Kuppelwieser, 2014). The specific tool used was Smart PLS 4 data analysis software to assess the measurement model and the structural model of the research model.

4.1 Measurement Model

All first-order constructs in the research model are reflective. Then, to evaluate their measurement models, the study will test the reliability, convergent, and discriminant validity (Hair Jr et al., 2014). The composite reliability (see Table 2) of the first-order constructs is all above the threshold value of 0.70, which indicates the internal consistency of the data (Fornell & Larcker, 1981). Several composite reliability values which fluctuate at 0.95, as suggested by Hair Jr et al. (2014), are acceptable. In addition, Hair Jr et al. (2014) suggests that item loadings of 0.7 are adequate; those with values lower than 0.7 (SEV3 and SEE1) were eliminated from the scales accordingly.

The convergent validity is assured when the value of AVE is above the threshold value of 0.5 (Hair Jr et al., 2014). Table 2 shows that the AVE ranged from approximately 0.5 to up. The result is acceptable as it indicates that a latent variable is able to explain about half of the variance of its indicator on average.

The discriminant validity is the degree to which a construct is distinguished from another by empirical criteria (Hair Jr et al., 2014). This study used the HTMT index (Heterotrait-montrait ratio) to evaluate the discriminant value. All first-order factors have HTMT index less than 0.85 (see Table 3), meaning that all sets of first-order scales have discriminant value (Ringle, Sarstedt, & Straub, 2012).

Besides, the second-order constructs in the research model are all formative, each of which represents a broader contextual factor that covaries with several underlying first-order factors (Chin, 1998). Second-order constructs are modeled at a higher or more abstract level, and their use is common (Chin, 1998). As shown in Table 4, the weight of each dimension to its designated constructs are significant ($p < 0.001$), and the VIF values are low, less than 3.33 (Diamantopoulos & Siguaw, 2006). Hence, formative models seem to be suitable.

In addition, Harman's single-factor test is performed to determine the possible degree of bias in the data sample. The results indicate that this study is not affected by common method bias problems.

4.2 Structural Model

The research model does not violate the multicollinearity phenomenon because the independent variables have VIF values < 2 compared to the corresponding dependent variable (Ringle et al., 2012).

Table 2. Reliability and convergent validity of reflective first-order constructs (reflective).

First-order construct	Indicators	Loading	Composite Reliability	AVE
Perceived severity (SEV)	SEV1	0.806	0.902	0.822
	SEV2	0.807		
Perceived vulnerability (VUL)	VUL1	0.843	0.888	0.726
	VUL2	0.907		
	VUL3	0.803		
Response efficacy (REE)	REE1	0.841	0.898	0.746
	REE2	0.876		
	REE3	0.874		
Self-efficacy (SEE)	SEE2	0.864	0.864	0.761
	SEE3	0.737		
Attitude (ATT)	ATT1	0.809	0.893	0.737
	ATT2	0.912		
	ATT3	0.852		
Subjective norms (SUB)	SUB1	0.926	0.962	0.833
	SUB2	0.925		
	SUB3	0.909		
	SUB4	0.931		
	SUB5	0.873		
Intention (INT)	INT1	0.872	0.936	0.830
	INT2	0.947		
	INT3	0.913		
Behavior (BEH)	BEH1	0.845	0.889	0.727
	BEH2	0.855		
	BEH3	0.858		
	BEH3	0.858		

The structural model results are described in Table 5. Hypotheses H_{2a}, H_{3a}, H_{3b}, H_{4b}, and H_5 have high path coefficients values at the significant level of 0.001, therefore, they are all accepted. In others words, coping appraisal of accounting information system security has a direct, positive and significant impact on AISSP compliance behaviors; attitude to comply with AISSP has a direct, positive and significant impact on AISSP compliance behaviors; attitude to comply with AISSP has a partially indirect, positive and significant impact on AISSP compliance behaviors through intention to comply with AISSP; intention to comply with AISSP fully mediates the effect of subjective norms on AISSP compliance behaviors; and intention to comply with ISSP has a positive and significant impact on AISSP compliance behaviors.

Table 3. Discriminant validity of first-order constructs according to HTMT index approach.

	BEH	INT	REE	SEE	SEV	SPA	SUN	VUL
BEH								
INT	0.602							
REE	0.578	0.227						
SEE	0.366	0.275	0.571					
SEV	0.295	0.054	0.395	0.201				
SPA	0.835	0.445	0.579	0.387	0.256			
SUB	0.371	0.452	0.257	0.243	0.138	0.252		
VUL	0.276	0.119	0.267	0.353	0.373	0.227	0.243	

Table 4. Validity of second-order constructs (formative).

Second-order constructs	First-order constructs	Weight	VIF
Threat appraisal	SEV	3.231***	1.314
	VUL	4.264***	1.342
Coping appraisal	REE	16.312***	1.328
	SEE	1.115***	1.327
*** $p < 0.001$, *$p < 0.1$			

All variables together account for 58.1% of the variance in the dependent construct. This information shows that the amount variance explained by the study's variables is fairly considerable (Chin, 1998), and is thus valuable to knowledge. To gain a greater understanding of the predictive capacity of PMT and TRA, separate analyses with each of the theory were performed on SmartPLS. The PMT model incorporates threat appraisal, coping appraisal, intention to comply AISSP and compliance behavior. The TRA model comprises of attitude, subjective norms, intention to comply AISSP and compliance behavior. The results revealed that the amount of variance explained by the constructs of PMT and TRA alone on the dependent variable is 43.2% and 51.5%, respectively. The result's analysis is described in the subsequent section.

5 Discussion

The result related to one of the PMT components, namely the coping appraisal, which has a direct positive effect on AISSP compliance behavior, confirms that employees are more likely to adopt their organization's AISSP if they have the relevant competence and capability regarding taking information security precautions and implementing preventive security measures; and employees' AISSP compliance behavior is enhanced when they believe that the expected returns are greater than the costs. The relationship is

Table 5. Research hypotheses test results.

H	Relationships	Std Beta	Std Error	[t-value]^	Conclusion	95% CI LL	95% CI UL
H_{1a}	Threat → BEH	0.076	0.044	1.743	No	-0.010	0.164
H_{1b}	Threat → INT → BEH	-0.016	0.015	1.018	No	-0.043	0.020
H_{2a}	Coping → BEH	0.142	0.062	2.283***	**Supported**	0.032	0.276
H_{2b}	Coping → INT → BEH	0.005	0.020	0.227	No	-0.028	0.052
H_{3a}	ATT → BEH	0.485	0.081	5.984***	**Supported**	0.310	0.627
H_{3b}	ATT → INT → BEH	0.084	0.038	2.190***	**Supported**	0.033	0.182
H_{4a}	SUB → BEH	0.054	0.062	0.870	No	-0.072	0.171
H_{4b}	SUB → INT → BEH	0.096	0.044	2.177***	**Supported**	0.031	0.201
H_5	INT → BEH	0.271	0.079	3.439***	**Supported**	0.149	0.456

*** $p < 0.001$; R2 (Intension = 0.263; Behavior = 0.581)

consistent with earlier research (Ifinedo, 2012; Johnston & Warkentin, 2010). However, the final component of PMT, the threat appraisal, was shown to have no link with both intention and compliance behavior with AISSP according to the study findings. This is somewhat unexpected as it is reasonable to anticipate that an individual's perception of risks, vulnerabilities, security breaches and assaults would inspire compliance with the organization's AISSP. This outcome may have been affected by external or contextual factors. It is also feasible that this component does not have a direct relationship with AISSP compliance behavior and that TRA's variables are not appropriate mediators in the context of this research.

Attitudes toward compliance from the TRA were shown to have significant direct and partially indirect positive impacts on AISSP compliance behavior while subjective norms also from TRA have a fully indirect influence on AISSP compliance behavior through intention to comply with AISSP. These findings suggest that an employees' attitude toward AISSP compliance in their businesses and the opinions of their coworkers play crucial roles in driving AISSP compliance behavior.

5.1 Implications for Research

This study offers implications to researchers. First, this research proposes and validates a research conceptualization that integrates PMT and TRA in the context of individuals or employees' AISSP compliance behavior. The findings of this research indicates that the fusion of both theoretical frameworks permits a better understanding of the sorts of factors that affect employees' AISSP compliance behavior as opposed to when each is used alone to investigate the theme. Second, this is the first time that threat appraisal and coping appraisal are considered higher-order constructs. Higher-order constructs are more general since they are measured at a high level of abstraction, while simultaneously assessing several sub-components (dimensions). Hence, by specifying lower-order components, higher-order constructs cover concrete traits of a more general conceptual variable of interest (Hult et al., 2018). Third, this current study lends credence to PMT and TRA, in so far as such factors as the coping appraisal (including the perception of one's capability (self-efficacy), response efficacy), attitude toward compliance, and subjective norms influence employees' AISSP compliance intention and behavior. Fourth, this research broadens our understanding of IS as well as AIS security practices in businesses from the view of accounting-function-related employees. Such considerations are crucial for boosting comprehension (Herath & Rao, 2009a; Ifinedo, 2012; Lee & Kozar, 2005). Finally, this study, along with others in the field, paves the way for creating a critical, integrated contingency model for measuring AISSP compliance in particular and ISSP compliance in general in businesses.

5.2 Implications for Practice

According to the findings of this research, management may improve AISSP compliance by ensuring that regular in-house IS/AIS security awareness sessions, campaigns, and training are provided to employees in order to mold their intentions and behaviors. Those who have incorrect attitudes about the AISSP may benefit from regular orientations and education. Because an individual's compliance with the AISSP can be influenced by superiors, peers, IS personnel, and other influential people in his or her immediate environment, management can ensure the success of their AISSP by identifying influential people in organizations capable of motivating or shaping the opinions of others and assigning them the responsibility of "championing" AISSP compliance in their respective contexts.

Given the importance of self-efficacy and response efficacy (also known as the coping appraisal) to AISSP compliance behavior, management may choose to expose employees to developing security technologies and encourage them to obtain the skills and knowledge necessary to protect organizational information systems assets. It is made much simpler to adhere to the IS/AIS security laws and regulations when there is encouragement for control and the development of skills.

5.3 Limitations of the Study and Future Research

This research has limits. Although the common method bias was not a concern for this research, participants may have supplied "socially desirable replies" (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Some of the study questionnaire's measuring questions and wordings may have been misconstrued by respondents, skewing their replies and affecting data analysis. This may affect the generalizability of the study's results. The sample was based on 226 informants. A higher sample size may give better statistical power and performance, even if the research concepts and analyses satisfied PLS standards (Chin, 1998).

This study focuses on employees' attitudes of AISSP compliance; future research might explore contractors and other personnel in this era of outsourcing. To expand our knowledge, we may compare workers' AISSP compliance practices in nations with strong and poor privacy rules. External determinants of employees' and other staff's AISSP compliance behavior and their probable consequences on rational worker behavior vis-à-vis response effectiveness need investigation. Very little study has been done on how to communicate AISSP without instilling fear, uncertainty and despair (FUD) in employees and staff.

6 Conclusion

This study was inspired by organizations' attempts to secure IS assets. Organizations occasionally buy tech to help them succeed, may then concentrate on implementing AISSP. Why needs regulations and guidelines if the staff not follow them? This study used PMT and TRA to expand understanding of the topic. Accounting-function-related employees were surveyed. The study found that coping appraisal (self-efficacy, response efficacy), attitude toward compliance, and subjective norms significantly directly/indirectly affected AISSP compliance intention and behavior. Our understanding of employees' AISSP compliance behavior in particular and ISSP compliance behavior in general is engendered by this research endeavor.

Appendix

Description of ISSP provided to the research's participants:

Information Systems Security Policy (ISSP) is often a formal and written document that provides precise regulations or guidelines that must be followed to protect the IS assets of an organization from intentional abuse or destruction; in other words, to maintain the integrity, confidentiality, and availability of information resources. For examples, ISSP typically describes practices related to the following: employees' responsibilities for protecting business information from potential security incidents, conducting information access control, downloading illegal software and freeware, utilizing anti-spyware, anti-virus tools, and firewalls, responding to spam emails, changing passwords at regular intervals, visiting suspicious websites, and storing sensitive information… Son (2011). ISSP is formal when it is explicitly defined or declared.

References

Ajzen, I.: The theory of planned behavior. Organizational behavior and human decision processes 50(2), 179-211 (1991).

Ajzen, I., Fishbein, M.: Belief, attitude, intention, and behavior: An introduction to theory and research. Philosophy and Rhetoric 10(2) (1975).

Ali, R. F., Dominic, P., Ali, S. E. A., Rehman, M., Sohail, A.: Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences 11(8), 3383 (2021).

Alias, R. A.: Information security policy compliance: Systematic literature review. Procedia Computer Science 161, 1216-1224 (2019).

Anderson, C. L., Agarwal, R.: Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS quarterly 34(3), 613-643 (2010).

Aurigemma, S.: A Composite Framework for Behavioral Compliance with Information Security Policies. Journal of Organizational and End User Computing 25, 32-51 (2013).

Bélanger, F., Collignon, S., Enget, K., Negangard, E.: Determinants of early conformance with information security policies. Information & Management 54(7), 887-901 (2017).

Blythe, J. M., Coventry, L.: Costly but effective: Comparing the factors that influence employee anti-malware behaviours. Computers in human behavior 87, 87-97 (2018).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., Polak, P.: 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 (2015).

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

Chan, M., Woon, I., Kankanhalli, A.: Perceptions of information security in the workplace: linking information security climate to compliant behavior. Journal of Information Privacy and Security 1(3), 18-41 (2005).

Chin, W. W.: Commentary: Issues and opinion on structural equation modeling. In (pp. vii-xvi): JSTOR (1998).

Davis, F. D., Bagozzi, R. P., Warshaw, P. R.: User acceptance of computer technology: A comparison of two theoretical models. Management science 35(8), 982-1003 (1989).

Diamantopoulos, A., Siguaw, J. A.: Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. British journal of management 17(4), 263-282 (2006).

Eveland, J.: Diffusion, technology transfer, and implementation: Thinking and talking about change. Knowledge 8(2), 303-322 (1986).

Ezzamel, M., Bourn, M.: The roles of accounting information systems in an organization experiencing financial crisis. Accounting, Organizations and Society 15(5), 399-424 (1990).

Fishbein, M., Ajzen, I.: Belief, attitude, intention, and behavior: An introduction to theory and research (1977).

Fishbein, M., Ajzen, I.: Understanding attitudes and predicting social behavior (1980).

Fornell, C., Larcker, D. F." Structural equation models with unobservable variables and measurement error: Algebra and statistics. In: Sage Publications Sage CA: Los Angeles, CA (1981).

Hair Jr, J. F., Sarstedt, M., Hopkins, L., Kuppelwieser, V. G.: Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. European business review (2014).

Herath, T., Rao, H. R.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems 47(2), 154-165 (2009).

Herath, T., Rao, H. R.: Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decision Support Systems 47, 10.1016 (2009a).

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

Hult, G. T. M., Hair Jr, J. F., Proksch, D., Sarstedt, M., Pinkwart, A., Ringle, C. M.: Addressing endogeneity in international marketing applications of partial least squares structural equation modeling. Journal of International Marketing 26(3), 1-21 (2018).

Ifinedo, P.: 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 (2012).

Ifinedo, P.: Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management 51(1), 69-79 (2014).

Johnston, A. C., Warkentin, M.: Fear appeals and information security behaviors: an empirical study. MIS quarterly, 549–566 (2010).

Knapp, K. J., Marshall, T. E., Rainer, R. K., Ford, F. N.: Information security: management's effect on culture and policy. Information management & computer security 14(1), 24-36 (2006).

Lebek, B., Uffen, J., Neumann, M., Hohler, B., H. Breitner, M.: Information security awareness and behavior: a theory-based literature review. Management Research Review 37(12), 1049–1092 (2014).

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

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

Milne, S., Sheeran, P., Orbell, S.: Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. Journal of Applied Social Psychology 30(1), 106-143 (2000).

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A.: What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems 18(2), 126-139 (2009).

Pahnila, S., Siponen, M., Mahmood, A.: Employees' behavior towards IS security policy compliance. Paper presented at the 2007 40th ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (HICSS'07) (2007a).

Pahnila, S., Siponen, M., & Mahmood, A.: Employees' behavior towards IS security policy compliance. Paper presented at the System sciences, 2007. HICSS 2007. 40Th ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (2007b).

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., Podsakoff, N. P.: Common method biases in behavioral research: a critical review of the literature and recommended remedies. Journal of applied psychology 88(5), 879 (2003).

Ringle, C. M., Sarstedt, M., Straub, D. W.: Editor's comments: a critical look at the use of PLS-SEM in" MIS Quarterly". MIS quarterly, iii-xiv (2012).

Rippetoe, P. A., & Rogers, R. W.: Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. Journal of personality and social psychology 52(3), 596 (1987).

Rogers, R. W.: A protection motivation theory of fear appeals and attitude change1. The journal of psychology 91(1), 93-114 (1975).

Rogers, R. W.: Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. Social psychophysiology: A sourcebook, 153–176 (1983).

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., Herawan, T.: Information security conscious care behaviour formation in organizations. Computers & Security 53, 65-78 (2015).

Safa, N. S., Von Solms, R., Furnell, S.: Information security policy compliance model in organizations. Computers & Security 56, 70-82 (2016).

Siponen, M., Mahmood, M. A., Pahnila, S.. Employees' adherence to information security policies: An exploratory field study. Information & management 51(2), 217-224 (2014).

Siponen, M., Pahnila, S., Mahmood, A.: Factors influencing protection motivation and IS security policy compliance. Paper presented at the 2006 Innovations in Information Technology (2006).

Siponen, M., Pahnila, S., Mahmood, M. A.: Compliance with information security policies: An empirical investigation. Computer 43(2), 64-71 (2010b).

Siponen, M., Vance, A.: Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 487–502 (2010).

Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J.: Variables influencing information security policy compliance: A systematic review of quantitative studies. Information management & computer security (2014).

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

Straub, D., Limayem, M., & Karahanna-Evaristo, E.: Measuring system usage: Implications for IS theory testing. Management science 41(8), 1328-1342 (1995).

T Alanazi, S., Anbar, M., A Ebad, S., Karuppayah, S., Al-Ani, H. A.: Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. Symmetry 12(9), 1544 (2020).

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

Venkatesh, V., Morris, M. G., Davis, G. B., Davis, F. D.: User acceptance of information technology: Toward a unified view. MIS quarterly, 425–478 (2003).

Warkentin, M., Siponen, M., Johnston, A. C.: An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. MIS quarterly 39, 113-134 (2015).

Woon, I., Tan, G.-W., Low, R.: A protection motivation theory approach to home wireless security. ICIS 2005 proceedings, 31, (2005).

Workman, M., Bommer, W. H., & Straub, D.: Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in human behavior 24(6), 2799-2816 (2008).

Yoon, C., Kim, H.: Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. Information Technology & People (2013).